Fuzzy Systems and Soft Computing
ISSN : 1819-4362

# FOUREYE DEFENSIVE DECEPTION AGAINST ADVANCED PERSISTENT THREATS VIA MACHINE LEARNING

**[1]P. Hrudhai, [2]G.Sri Soumya, [3]D. Sathwik, [4]K. Pushkar, [5]Vinod Gendre**

**[1,2,3,4]UG Scholar, Department of CSE (AI&ML)**

**[5]Assistant Professor, Department of CSE (AI&ML)**

**CMR Institute of Technology, Hyderabad, Telangana, India-501401**

## ABSTRACT

Defensive deception techniques have emerged as a promising proactive defense mechanism to mislead an attacker and thereby achieve attack failure. However, most game-theoretic defensive deception approaches have assumed that players maintain consistent views under uncertainty. They do not consider players' possible, subjective beliefs formed due to asymmetric information given to them. In this work, we formulate a hypergame between an attacker and a defender where they can interpret the same game differently and accordingly choose their best strategy based on their respective beliefs. This gives a chance for defensive deception strategies to manipulate an attacker's belief, which is the key to the attacker's decision making. We consider advanced persistent threat (APT) attacks, which perform multiple attacks in the stages of the cyber kill chain where both the attacker and the defender aim to select optimal strategies based on their beliefs. Through extensive simulation experiments, we demonstrated how effectively the defender can leverage defensive deception techniques while dealing with multi-staged APT attacks in a hypergame in which the imperfect information is reflected based on perceived uncertainty, cost, and expected utilities of both attacker and defender, the system lifetime (i.e., mean time to security failure), and improved false positive rates in detecting attackers

**INTRODUCTION:**The key purpose of a defensive deception technique is to mislead an attacker's view and make it choose a suboptimal or poor action for the attack failure [33]. When both the attacker and defender are constrained in their resources, strategic interactions can be the key to beat an opponent. In this sense, non-game-theoretic defense approaches have inherent limitations due to lack of efficient and effective strategic tactics. Forms of deception techniques have been discussed based on certain classifications, such as hiding the truth vs. providing false information or passive vs. active for increasing attackers' ambiguity or confusion [3, 9].Game theory has been substantially used for dynamic decision making under uncertainty, assuming that players have

http://doi.org/10.36893/FSCC.2024.V09I01.049-058

consistent views. However, this assumption fails as players may often subjectively process asymmetric information available to them [22]. Hyper game theory [5] is a variant of game theory that provides a form of analysis considering each player's subjective belief, misbelief, and perceived uncertainty and accordingly their effect on decision making in choosing a best strategy [22]. This paper leverages hyper game theory to resolve conflicts of views of multiple players as a robust decision making mechanism under uncertainty where the players may have different beliefs towards the same game. Hyper game theory models players, such as attackers and defenders in cyber security to deal with advanced persistent threat (APT) attacks. We dub this effort Foureye after the Foureye butterfly fish, demonstrating deceptive defense in nature [40].To be specific, we identify the following nontrivial challenges in obtaining a solution. First of all, it is not trivial to derive realistic game scenarios and develop defensive deception techniques to deal with APT attacks beyond thereconnaissance stage. This aspect has not been explored in the state-of-the-art. Second, quantifying the degree of uncertainty in the views of attackers and defenders is challenging, although they are critical because how each player frames a game significantly affects its strategies to take. Third, given a number of possible choices under dynamic situations, dealing with a large number of solution spaces is not trivial whereas the deployment and maintenance of defensive deception techniques is costly in contested environments. We partly addressed these challenges in our prior work in [12]; however, its contribution is very limited in considering a small-scale network and a small set of strategies with a highly simplified probability model developed using Stochastic Petri Network.

To be specific, this paper has the following **new key contributions**:

- We modeled an attack-defense game under uncertainty based on hypergame theory where an attacker and a defender have different views of the situation and are uncertain about strategies taken by their opponents.
- We reduced a player's action space by using a sub game determined based on a set of strategies available where each sub game is formulated based on each stage of the cyber kill chain (CKC) based on a player's belief under uncertainty.
- We considered multiple defense strategies, including defensive deception techniques whose performance can be significantly affected by an attacker's belief and perceived uncertainty, which impacts its choice of a strategy.

http://doi.org/10.36893/FSCC.2024.V09I01.049-058

- We modeled an attacker's and a defender's uncertainty towards its opponent (i.e., the defender and the attacker, respectively) based on how long each player has monitored the opponent and its chosen strategy. To the best of our knowledge, prior research on hyper game theory uses a predefined constant probability to represent a player's uncertainty. In this work, we estimated the player's uncertaintybased on the dynamic, strategic interactions between an attacker and a defender.
- We conducted comparative performance analysis with or without a defender using defensive deception (DD) strategies and with or without perfect knowledge available towards actions taken by the opponent. We measured the effectiveness and efficiency of DD techniques in terms of a system's security and performance, such as perceived uncertainty, hyper game expected utility, action cost, mean time to security failure (MTTSF or system lifetime), and improved false positive rate (FPR) of an intrusion detection by the DD strategies taken by the defender.

**RELATED WORK**

Garg and Grosu [15] proposed a game-theoretic deceptionframework in honeynets with imperfect informationto find optimal actions of an attacker and a defender andinvestigated the mixed strategy equilibrium. Carroll andGrosu [10] used deception in attacker-defender interactionsin a signaling game based on perfect Bayesian equilibriaand hybrid equilibria. They considered defensive deceptiontechniques, such as honeypots, camouflaged systems, ornormal systems. Yin et al. [41] considered a Stackelbergattack-defense game where both players make decisionsbased on their perceived observations and identified anoptimal level of deceptive protection using fake resources.Casey et al. [11] examined how to discover Sybil attacksbased on an evolutionary signaling game where a defendercan use a fake identity to lure the attacker to facilitatecooperation. Schlenker et al. [32] studied a sophisticated andna¨ıve APT attacker in the reconnaissance stage to identify anoptimal defensive deception strategy in a zero-sum Stackelberggame by solving a mixed integer linear program.Unlike the above works cited [10, 11, 15, 32, 41], ourwork used hypergame theory which offers the powerful capabilityto model uncertainty, different views, and boundedrationality by different players. This way reflects more realisticscenarios between the attacker and defender.Hypergame theory has emerged to better reflect realworldscenarios by

http://doi.org/10.36893/FSCC.2024.V09I01.049-058

capturing players' subjective and imperfectbelief, aiming to mislead them to adopt uncertainor non-optimized strategies. Although other game theoriesdeal with uncertainty by considering probabilities that acertain event may happen, they assume that all players playthe same game [34]. Hypergame theory has been used tosolve decision-making problems in military and adversarialenvironments House and Cybenko [20], Vane [37], Vaneand Lehner [39]. Several studies [16, 17] investigated howplayers' beliefs evolve based on hypergame theory by developinga misbelief function measuring the differencesbetween a player's belief and the ground truth payoff ofother players' strategies. Kanazawa et al. [21] studied anindividual's belief in an evolutionary hypergame and howthis belief can be modelled by interpreter functions. Sasaki[31] discussed the concept of subjective rationalizability wherean agent believes that its action is a best response to theother agent's choices based on its perceived game.Putro et al. [30] proposed an adaptive, genetic learningalgorithm to derive optimal strategies by players in a hypergame.Ferguson-Walter et al. [13] studied the placementof decoys based on a hypergame. This work developed agame tree and investigated an optimal move for both anattacker and defender in an adaptive game. Aljefri et al.[2] studied a first level hypergame involving misbeliefs toresolve conflicts for two and then more decision makers.Bakker et al. [4] modeled a repeated hypergame in dynamicstochastic setting against APT attacks primarily in cyberphysicalsystems.Unlike the works using hypergame theory above [2,4, 13, 16, 17, 20, 21, 30, 31, 37, 39], our work consideredan APT attacker performing multi-staged attacks whereattack-defense interactions are modeled based on repeatedhypergames. In addition, we show the effectiveness of defensivedeception techniques by increasing the attacker'suncertainty leading to choosing non-optimal actions andincreasing the quality of the intrusion detection (i.e., anetwork-based intrusion detection system, NIDS) throughthe collection of attack intelligence using defensive deceptionstrategies.

**EXISTING SYSTEM**

Garg and Grosu [15] proposed a game-theoretic deception framework in honeynets with imperfect information to find optimal actions of an attacker and a defender and investigated the mixed strategy equilibrium. Carroll and Grosu [10] used deception in attacker-defender interactions in a signaling game based on perfect Bayesian equilibria and hybrid equilibria. They considered defensive deception techniques, such as honeypots, camouflaged systems, or normal systems. Yin et al. [41] considered a Stackelberg attack-defense game where both

http://doi.org/10.36893/FSCC.2024.V09I01.049-058

players make decisions based on their perceived observations and identified an optimal level of deceptive protection using fake resources. Casey et al. [11] examined how to discover Sybil attacks based on an evolutionary signaling game where a defender can use a fake identity to lure the attacker to facilitate cooperation. Schlenker et al. [32] studied a sophisticated and na¨ıve APT attacker in the reconnaissance stage to identify an optimal defensive deception strategy in a zero-sum Stackelberg game by solving a mixed integer linear program. Unlike the above works cited [10, 11, 15, 32, 41], our work used hypergame theory which offers the powerful capability to model uncertainty, different views, and bounded rationality by different players. This way reflects more realistic scenarios between the attacker and defender. Hypergame theory has emerged to better reflect realworld scenarios by capturing players' subjective and imperfect belief, aiming to mislead them to adopt uncertain or non-optimized strategies. Although other game theories deal with uncertainty by considering probabilities that a certain event may happen, they assume that all players play the same game [34]. Hypergame theory has been used to solve decision-making problems in military and adversarial environments House and Cybenko [20], Vane [37], Vane and Lehner [39]. Several studies [16, 17] investigated how players' beliefs evolve based on hypergame theory by developing a misbelief function measuring the differences between a player's belief and the ground truth payoff of other players' strategies. Kanazawa et al. [21] studied an individual's belief in an evolutionary hypergame and how this belief can be modelled by interpreter functions. Sasaki [31] discussed the concept of subjective rationalizability where an agent believes that its action is a best response to theother agent's choices based on its perceived game. Putro et al. [30] proposed an adaptive, genetic learning algorithm to derive optimal strategies by players in a hypergame. Ferguson-Walter et al. [13] studied the placement of decoys based on a hypergame. This work developed a game tree and investigated an optimal move for both an attacker and defender in an adaptive game. Aljefri et al. [2] studied a first level hypergame involving misbeliefs to resolve conflicts for two and then more decision makers.Bakker et al. [4] modeled a repeated hypergame in dynamistochastic setting against APT attacks primarily in cyberphysicalsystems.

**DISADVANTAGES**

- The system can't track attack which can be performed to exploit unknown vulnerabilities of software, which are not patched yet.
- The system can't track Fake identity attack which can be performed when

http://doi.org/10.36893/FSCC.2024.V09I01.049-058

packets are transmitted without authentication or internal nodes spoofing the ID of a source node

**PROPOSED SYSTEM**

- The system modeled an attack-defense game under uncertainty based on hypergame theory where an attacker and a defender have different views of the situation and are uncertain about strategies taken by their opponents.
- The system reduced a player's action space by using a subgame determined based on a set of strategies available where each subgame is formulated based on each stage of the cyber kill chain (CKC) based on a player's belief under uncertainty.
- The system considered multiple defense strategies, including defensive deception techniques whose performance can be significantly affected by an attacker's belief and perceived uncertainty, which impacts its choice of a strategy.
- The system modeled an attacker's and a defender's uncertainty towards its opponent (i.e., the defender and the attacker, respectively) based on how long each player has monitored the opponent and its chosen strategy. To the best of our knowledge, prior research on hypergame theory uses a predefined constant probability to represent a player's uncertainty. In this work, we estimated the player's uncertainty based on the dynamic, strategic interactions between an attacker and a defender.
- The system conducted comparative performance analysis with or without a defender using defensive deception (DD) strategies and with or without perfect knowledge available towards actions taken by the opponent. We measured the effectiveness and efficiency of DD techniques in terms of a system's security and performance, such as perceived uncertainty, hypergame expected utility, action cost, mean time to security failure (MTTSF or system lifetime), and improved false positive rate (FPR) of an intrusion detection by the DD strategies taken by the defender.

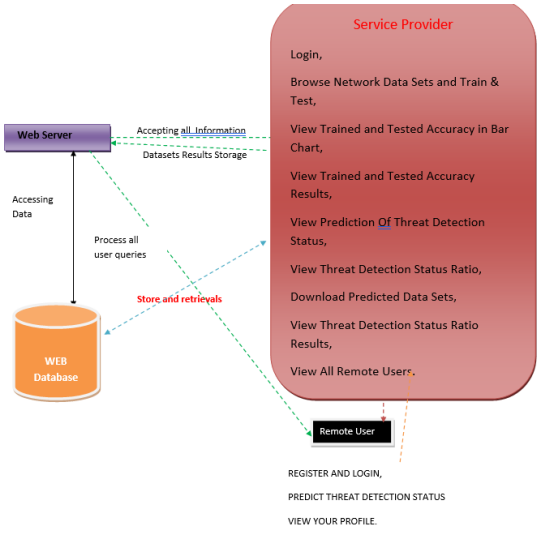
**ADVANTAGES**

- APT Attack Procedure to Achieve Data Exfiltration in which the system define an APT attacker's goal in that the attacker has reached and compromised a target node and successfully exfiltrated its confidential data.
- The system proposed many ML

http://doi.org/10.36893/FSCC.2024.V09I01.049-058

Classifiers to test and train the different types of attacks and can be predicted by using same classifiers.

## IMPLEMENTATION




## MODULES

### Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse Network Data Sets and Train & Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Threat Detection Status, View Threat Detection Status Ratio, Download Predicted Data Sets, View Threat Detection Status Ratio Results, View All Remote Users.

**View and Authorize Users**In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

**Remote User**In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN,PREDICT THREAT DETECTION STATUS,VIEW YOUR PROFILE.

## CONCLUSION

From this study, we obtained the following **key findings**:

- An attacker's and defender's perceived uncertainty can be reduced when defensive deception (DD) is used. This is because the attacker perceives more knowledge about the system as it performs attacks as an inside attacker. On the other hand, the defender's uncertainty can be reduced by collecting more attack intelligence by using DD while allowing the attacker to be in the system.
- Attack cost and defense cost are two critical factors in determining HEUs (hyper game expected utilities). Therefore, high DHEU (defender's HEU) is not necessarily related to

http://doi.org/10.36893/FSCC.2024.V09I01.049-058

high system performance in MTTSF (mean time to security failure) or TPR (true positive rate) which can also be a key indicator of system security. Therefore, using DD under imperfect information (IPI) yields the best performance in MTTSF (i.e., the longest system lifetime) while it gives the minimum DHEU among all schemes.

- DD can effectively increase TPR of the NIDS in the system based on the attack intelligence collected through the DD strategies.

This work bring up some important directions for future research by: (1) considering multiple attackers arriving in a system simultaneously in order to consider more realistic scenarios; (2) estimating each player's belief based on machine learning in order to more correctly predict a next move of its opponent; (3) dynamically adjusting a risk threshold, i.e., Eq. (6), depending on a system's security state; (4) introducing a recovery mechanism to restore a compromised node to a healthy node allowing the recovery delay; (5) developing an intrusion response system that can reassess a detected intrusion in order to minimize false positives while identifying an optimal response strategy to deal with intrusions with high urgency; and (6) considering another intrusion prevention mechanism, such as moving target defense, as one of the defense strategies.

**REFERENCES**

[1] "Common vulnerability scoring system (CVSS)."[Online]. Available: https://www.first.org/cvss/

[2] Y. M. Aljefri, M. A. Bashar, L. Fang, and k. W. Hipel,"First-level hypergame for investigating misperceptionin conflicts," IEEE Trans. Systems, Man, and Cybernetics:Systems, vol. 48, no. 12, pp. 2158–2175, 2017.

[3] H. Almeshekah and H. Spafford, "Cyber security deception,"in Cyber Deception. Springer, 2016, pp. 25–52.

[4] C. Bakker, A. Bhattacharya, S. Chatterjee, and D. L.Vrabie, "Learning and information manipulation: Repeatedhypergames for cyber-physical security," IEEEControl Systems Letters, vol. 4, no. 2, pp. 295–300, 2019.

[5] P. G. Bennett, "Toward a theory of hypergames,"Omega, vol. 5, no. 6, pp. 749–751, 1977.

[6] E. Bertino and N. Islam, "Botnets and Internet of Thingssecurity," Computer, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[7] M. Boussard, D. T. Bui, L. Ciavaglia, R. Douville, M. L.Pallec, N. L. Sauze, L. Noirie, S. Papillon, P. Peloso,and F. Santoro, "Software-defined LANs for interconnectedsmart environment," in 2015

27th Int'l TeletrafficCongress, Sep. 2015, pp. 219–227.

[8] U. Brandes, "A faster algorithm for betweenness centrality,"Jour. mathematical sociology, vol. 25, no. 2, pp.163–177, 2001.

[9] J. W. Caddell, "Deception 101-primer on deception,"DTIC Document, Tech. Rep., 2004.

[10] T. E. Carroll and D. Grosu, "A game theoretic investigationof deception in network security," Security andCommunication Networks, vol. 4, no. 10, pp. 1162–1172,2011.

[11] W. Casey, A. Kellner, P. Memarmoshrefi, J. A. Morales,and B. Mishra, "Deception, identity, and security: Thegame theory of Sybil attacks," Comms. of the ACM,vol. 62, no. 1, pp. 85–93, 2018.

[12] J.-H. Cho, M. Zhu, and M. P. Singh, Modeling andAnalysis of Deception Games based on Hypergame Theory.Cham, Switzerland: Springer Nature, 2019, ch. 4, pp.49–74.

[13] K. Ferguson-Walter, S. Fugate, J. Mauger, and M. Major,"Game theory for adaptive defensive cyber deception,"in Proc. 6th Annual Symp. on Hot Topics in the Science ofSecurity. ACM, 2019, p. 4.

[14] N. M. Fraser and K. W. Hipel, Conflict Analysis: Modelsand Resolutions. North-Holland, 1984.

[15] N. Garg and D. Grosu, "Deception in honeynets: Agame-theoretic analysis," in Proc. IEEE Information Assuranceand Security Workshop (IAW). IEEE, 2007, pp.107–113.

1. S.Dhanalakshmi,,A.Indhuraj, V.Arunraj, and L.R.Angeeth, "A Survey of Different Image Segmentation Techniques and K-Means Algorithm", in International Journal of Software & Hardware Research in Engineering (IJSHRE), Volume 3, Issue 3, ISSN: 2347-4890,March 2015, PP 33-36
2. S.Dhanalakshmi,, and J.Ramya, "An Efficient Rain Detection and Removal from Videos using Rain Pixel Recovery Algorithm", in International Journal of Engineering Research Technology(IJERT), Volume 3, Issue 15,ISSN: 2278-0181,March 2015, PP 25-27
3. S.Dhanalakshmi,, "Achieving Privacy Preserved Content Retrieval with Assured Rank Integrity", in International Journal of Engineering Research Technology(IJERT), ISSN: 2278-0181, March 2015, Volume 3, Issue 15,,PP 28-31
4. S.Dhanalakshmi,, and K.Santhiosh, "Guaranteed Top K Retrieval of Contents Over Encrypted Cloud Data Using Fried Rank Man Testing", in International Journal of Applied Engineering Research Technology(IJAER), Volume 10,No.41,ISSN: 0973-4562, June 2015, PP 30449-30453 (SCOPUS/Annexure-II Journals)

.Reddy, Kumbala Pradeep, Sarangam Kodati, Madireddy Swetha, M. Parimala, and S. Velliangiri. "A hybrid neural network architecture for early detection of DDOS attacks using deep learning models." In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 323-327. IEEE, 2021.

4.Kodati, Sarangam, et al. "Analysis of Heart Disease Data Using K-Means Clustering Algorithm in Orange Tool." *Intelligent Manufacturing and Energy Sustainability:*

*Proceedings of ICIMES 2020*. Springer Singapore, 2021.

5.Reddy, Kumbala Pradeep, Gullipalli Apparao Naidu, and Bulusu Vishnu Vardhan. "View-Invariant Feature Representation for Action Recognition under Multiple Views." *International Journal of Intelligent Engineering & Systems* 12.6 (2019).

http://doi.org/10.36893/FSCC.2024.V09I01.049-058