International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at :www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET2512314

Defensive Deception Based on Hyper Game Theory against Advanced Persistent Threats

Shaik Mabu Basha, Banala Laxmi Venkata Sai Akhil, Boya Akhil, Rajala Madhusudhan Reddy, Dr. Tippanna

Department of Artificial Intelligence and Machine Learning, Dr K V Subba Reddy Institute of Technology, Kurnool, Andhra Pradesh, India

ARTICLEINFO

Article History:

Accepted : 05 May 2025
Published: 09 May 2025

Publication Issue :
Volume 12, Issue 3
May-June-2025

Page Number :
65-71

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 a symmetric information given to them. In this work, we formulate a hyper game 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 killchain 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 tosecurity failure), and improved false positive rates indetecting attackers.

INTRODUCTION

The key purpose of adefensivedeceptiontechniqueistomislead an attacker's view and make it choose a suboptimal or poor action for the attack failure. When both the attacker and defender are constrained in their resources, strategicinteractionscanbethekeytobeatanopponent.In thissense, 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 thetruthvs.providingfalse information or passive vs. active for increasing attackers' ambiguity or confusion.

Game theory has been substantially used for dynamic decision making underuncertainty,assumingthatplayershaveconsistent views.However,this assumption fails as players may often subjectively process asymmetric information available tothem.Hypergametheoryisavariantofgametheorythat providesaform of analysis considering each player's subjective belief, misbelief, and perceived uncertainty and accordingly their effect on decision making in choosing a best strategy. This paper leverages hyper game theory to resolve conflicts of views of multiple players as a robust decision makingmechanismunderuncertaintywherethe players may have different beliefs towards the same game. Hyper game theorymodels players, such as attackers and defenders in cyber security to deal with advanced persistent threat (APT) attacks. We dub this effort Foureye after theFoureye butterfly fish, demonstrating deceptive defense in nature.

Tobespecific,weidentifythefollowingnontrivialchalle ngesin obtaining a solution. First of all, it isnottrivialtoderiverealisticgamescenariosand develop defensive deception techniques to deal with APT attacks beyond the reconnaissancestage.Thisaspecthasnotbeenexploredin thestate-of-the-art.Second, quantifying the degree of uncertainty intheviewsofattackersanddefenders 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, dealingwithalargenumberofsolutionspacesisnottrivial whereas the deployment and maintenance of defensivedeceptiontechniquesiscostly in contested environments. We partly addressed these challenges in our prior work; 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.

Tobespecific,thispaperhasthefollowingnewkeycontrib utions:

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 reducedaplayer'sactionspacebyusingasubgamedetermi nedbasedonasetof 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 besignificantlyaffectedbyanattacker'sbeliefandperceiv ed uncertainty, which impacts its choice of a strategy.

We modeled an attacker's and a defender's uncertaintytowardsitsopponent(i.e.,the defender and the attacker,respectively)basedonhowlongeachplayerhas monitored the opponent and its chosen strategy. To the best ofourknowledge,priorresearchon hyper game theory uses a predefined constant probability to represent a player's uncertainty. Inthiswork,weestimatedtheplayer'suncertaintybasedo nthedynamic, 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 perfectknowledgeavailable towardsactionstakenbytheopponent.Wemeasuredthee ffectivenessand efficiencyof DD techniques in terms of a system's securityandperformance,suchasperceived

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.

Existing System

Garg and Grosu 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 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 ,considered a Stackelberg attack-defense game where both players make decisions based on their perceived observations and identified an optimal level of deceptive protection using fake resources.

Casey et al. 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 facilitatecooperation.Schlenkeretal.studiedasophisticatedandna¨ıveAPTattacker 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, our work used hypergame theory which offers the powerful capability to model uncertainty, different views, andboundedrationalityby different players. This way reflects more realistic scenarios between the attacker and defender.

Hypergame theory has emerged to better reflect real world scenarios by capturing players' subjective and imperfectbelief,aimingtomisleadthemtoadoptuncertainor non-optimized strategies. Although other game theories deal with uncertainty by consideringprobabilities that a certain event may happen, they assume that all playersplay the same game. Hypergame theory has been used to solve decision-making problems in military and adversarial environments House and Cybenko, Vane , Vaneand Lehner. Several studies 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.studiedanindividual'sbeliefinanevolutionaryhypergameandhow this belief can be modelled by interpreter functions. Sasaki discussed the concept of subjective rationalizability whereanagentbelievesthatitsactionisabestresponseto the other agent's choices based on its perceived game.Putro et al. proposed an adaptive, genetic learning algorithm to derive optimal strategies by players in ahypergame.Ferguson-Walteretal.studiedtheplacementof decoys based on a hypergame. This work developed a game tree and investigatedan optimal move for both an attacker and defender in an adaptive game. Aljefri et al. studied a first level hypergame involving misbeliefs to resolve conflicts for two and then more decision makers.Bakker et al. modeled a repeated hypergame in dynamic stochastic setting against APT attacks primarily in cyber physical systems.

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 performedwhenpackets aretransmitted 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 hypergametheory where an attacker and a defender have different views of the

situation and are uncertain about strategies taken by their opponents.

Thesystemreduced 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.

Thesystemconsideredmultipledefensestrategies,includingdefensivedeceptiontechniques 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 monitoredthe opponent and its chosen strategy. To the best of our knowledge, prior research on hypergame theory uses a predefined constant probability torepresentaplayer'suncertainty. 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 theopponent.Wemeasuredtheeffectivenessandefficiencyof 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

- APTAttackProceduretoAchieveDataExfiltrationinwhichthesystemdefineanAPT attacker's goal in that the attacker has reached and compromised a target node and successfully exfiltrated its confidential data.

Thesystem proposed manyML Classifiers totest and trainthe different typesof attacks.

Literature Survey

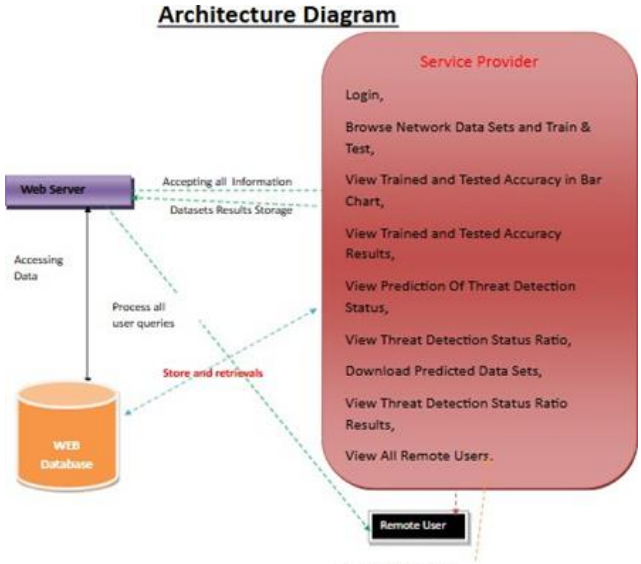
Defensive deception based on hypergame theory against Advanced Persistent Threats (APT) is an advanced cybersecurity strategy where defenders use strategic misinformation andperceptionmanipulationtomisleadsophisticatedattackerswhooperatewithpersistence and stealth.

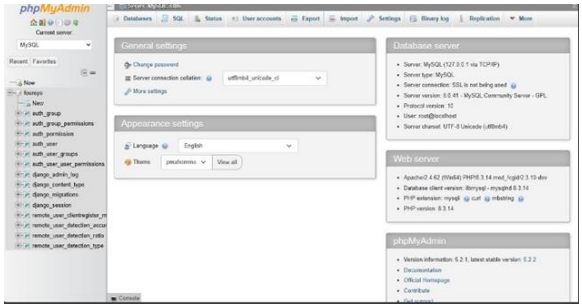
Hypergame theory extends traditional game theory by allowing players to have different perceptionsofthegametheyareplaying.It'sparticularlyusefulinconflictscenarioswhere deception, misinformation, or hidden intentions are at play.

Architecture

The system architecture is built around a centralized web-based platform that facilitates defensive deception and threat detection through hypergame-theoretic modeling. The architecture includesboth Service Provider and Remote User components. The Web Server functions as the primary interface, accepting user inputs and coordinating the flow of information. It interacts with a Web Database, responsible for storing and retrieving datasets, trained models, prediction results, and user profiles.Users,uponregistrationandlogin,canbrowsenetwork-relateddatasets,initiatetrainingand testing processes, and view threat detection predictions along with their associated accuracy metrics displayed in bar charts and result tables. These predictions are based on behavioral analysis and popularity metrics, helping to identify potential threat actors. Additionally, users can explore popularity prediction types and their ratios, which are crucial for modeling attacker belief states in hypergames. The system also features Tweet Servers that act as input feeds, possibly simulating or analyzing social media-driven threat vectors. All predicted and tested data can be downloaded for offlineanalysis.Thearchitecturesupportsreal-timevisualizationofthreatdetectionstatusesanduser interaction histories, which can be leveraged to mislead or trap sophisticated APT actors through

strategic misinformation. This dynamic, user-centric approach makes the architecture both scalable and effective in modeling misperception—a key principle of hypergame theory applied in modern cyber defense.





SYSTEM REQUIREMENTS

SoftwareRequirements

Operating system:Windows7 Ultimate.

Coding Language:Python.

Front-End:Python.

Back-End:Django-ORM

Designing:Html, CSS, JavaScript.

Data Base:MySQL(WAMPServer)

HardwareRequirements

Processor:Pentium -IV

RAM:4GB (min)

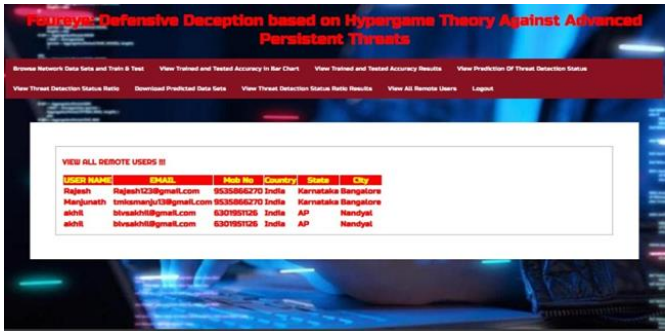
Hard Disk:20GB.

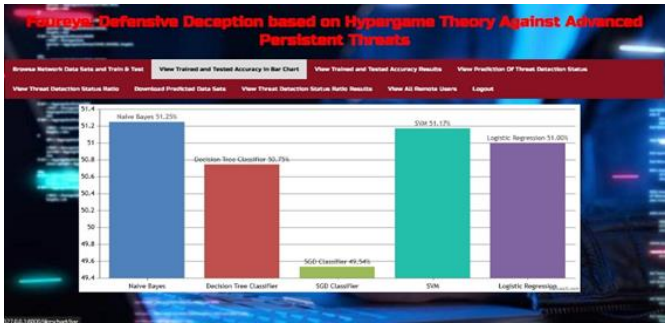
Keyboard:StandardWindows Keyboard

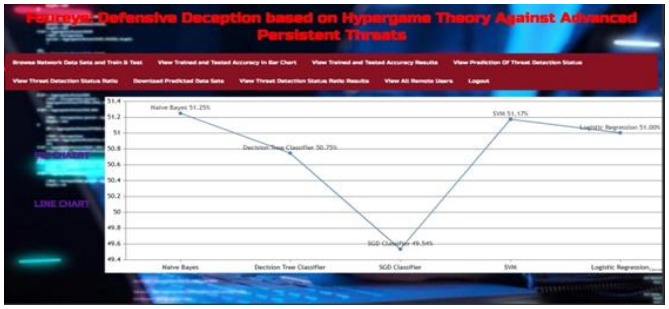
Mouse:TwoorThreeButtons Mouse

Monitor:SVGA

RESULT







CONCLUSION

Fromthisstudy,weobtainedthefollowingkey 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 reducedbycollectingmoreattackintelligencebyusingD Dwhileallowingtheattackertobein 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 high system performanceinMTTSF(meantimetosecurityfailure)orT PR(truepositiverate)whichcanalso 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.

DDcaneffectivelyincreaseTPRoftheNIDSinthesystem basedontheattackintelligence collected through the DD strategies.

This work bring up some important directions for future research by:

(1) consideringmultipleattackersarrivinginasystemsi multaneouslyinordertoconsidermore realistic scenarios;
(2) estimatingeachplayer'sbeliefbasedonmachinelear ninginordertomorecorrectlypredicta next move of its opponent;
(3) dynamicallyadjustingariskthreshold,i.e.,dependin gonasystem'ssecuritystate;
(4) introducingarecoverymechanismtorestoreacomp romisednodetoahealthynodeallowing the recovery delay; developing an intrusion response system that can reassess a detected intrusion in order to minimizefalsepositiveswhileidentifyinganoptima lresponsestrategytodealwithintrusions with high urgency;

REFERENCES

[1]. "Commonvulnerabilityscoringsystem(CVSS)."[Online].Available: https://www.first.org/cvss/

[2]. Y.M.Aljefri,M.A.Bashar,L.Fang,andk.W.Hipel," First-levelhypergame forinvestigatingmisperceptioninconflicts,"IEEE Trans.Systems,Man,and Cybernetics: Systems, vol. 48, no. 12, pp. 2158–2175, 2017.

[3]. H.AlmeshekahandH.Spafford,"Cybersecurityde ception," in Cyber Deception. Springer, 2016, pp. 25–52.

[4]. C. Bakker, A. Bhattacharya, S. Chatterjee, and D. L.Vrabie, "Learning and informationmanipulation:Repeatedhypergames forcyber-physicalsecurity," IEEE Control Systems Letters, vol. 4, no. 2, pp. 295–300, 2019.

[5]. P.G.Bennett,"Towardatheoryofhypergames,"O mega,vol.5,no.6,pp. 749–751, 1977.

[6]. E.BertinoandN.Islam,"BotnetsandInternetofThi ngssecurity,"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.PelosoandF.Santoro,"Soft ware-definedLANsfor interconnected smart environment," in 2015 27th Int'l Teletraffic Congress, Sep. 2015, pp. 219–227.

[8]. U.Brandes,"Afasteralgorithmforbetweennessce ntrality,"Jour.mathematical sociology, vol. 25, no. 2, pp.163–177, 2001.

[9]. J.W.Caddell,"Deception101-primerondeception,"DTICDocument,Tech. Rep., 2004.T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in networksecurity,"SecurityandCommunication Networks,vol.4,no.10,pp. 1162–1172,2011.

[10]. W.Casey, A. Kellner, P. Memarmoshrefi, J. A. Morales,and B. Mishra, "Deception,identity,andsecurity:Thegametheoryof Sybilattacks,"Comms. of the ACM, vol. 62, no. 1, pp. 85–93, 2018.

[11]. J.-H.Cho,M.Zhu,andM.P.Singh,ModelingandAnalysisofDeception GamesbasedonHypergameTheory.Cham,Switzerland:SpringerNature, 2019, ch. 4, pp.49–74.

[12]. K. Ferguson-Walter, S. Fugate, J. Mauger, and M. Major, "Game theory for adaptive defensivecyberdeception,"inProc.6thAnnualSymp.onHotTopicsintheScienceof Security. ACM, 2019, p. 4.

[13]. N.M.FraserandK.W.Hipel,ConflictAnalysis:ModelsandResolutions.North-Holland, 1984.

[14]. N.GargandD.Grosu,"Deceptioninhoneynets:A game-theoreticanalysis,"inProc.IEEE Information Assurance and Security Workshop (IAW). IEEE, 2007, pp.107–113.

[15]. B. Gharesifard and J. Cort´es, "Evolution of the perception about the opponent in hypergames,"inProc.49thIEEEConf.DecisionandControl(CDC),Dec.2010,pp. 1076–1081.

[16]. "Evolutionofplayers'misperceptionsinhypergamesunderperfectobservations,"IEEE Trans. Automatic Control, vol. 57, no. 7, pp. 1627–1640, Jul. 2012.

[17]. I.GmbH.MindNode.[Online].Available:https://mindnode.com/

[18]. Jangid, J., & Malhotra, S. (2022). Optimizing software upgrades in optical transport networks: Challenges and best practices. Nanotechnology Perceptions, 18(2), 194–206. https://nano-ntp.com/index.php/nano/article/view/5169

[19]. Dixit, S. (2022). AI-powered risk modeling in quantum finance: Redefining enterprise decision systems. International Journal of Scientific Research in Science, Engineering and Technology, 9(4), 547–572. https://doi.org/10.32628/IJSRSET221656

[20]. J.Han,J.Pei,andM.Kamber,DataMining:ConceptsandTechniques.Elsevier, 2011.

[21]. J. T. House and G. Cybenko, "Hypergame theory applied to cyber attack and defense," in Proc. SPIE Conf.Sensors, and Command, Control, Comms., and Intelligence (C3I) TechnologiesforHomelandSecurityandHomelandDefenseIX,vol.766604,May.2010.

[22]. T.Kanazawa, T. Ushio, and T. Yamasaki, "Replicator dynamics of evolutionary hypergames," IEEE Trans.Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 37, no. 1, pp. 132–138, Jan. 2007.

[23]. N.S.Kovach,A.S.Gibson,andG.B.Lamont,"Hypergametheory:Amodelforconflict, misperception, and deception," Game Theory, 2015, article ID 570639,20 pages.

[24]. K.Krombholz,H.Hobel,M.Huber,andE.Weippl," Advancedsocialengineeringattacks," Jour. Information Security and Applications, vol. 22, pp. 113–122, 2015.