Pegem Journal of Education and Instruction, Vol. 13, No. 3 , 2023 (pp. 489-503)

RESEARCH ARTICLE WWW.PEGEGOG.NET

Using Hyper game Theory for Defensive Deception Against Advanced Persistent Threats: Four Eye

[1]*DR. M. RAMASUBRAMANIAN*, [2]*SUNKARA SHREE SHREYA*, [3]*KUMMARI BHAVANA*, [4]*AKINA DIVYA*

[1]Professor, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

Email: ramanmass01@gmail.com

[2,3,4,]B.Tech Student, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

ABSTRACT

Emerging as a potential proactive defense mechanism, defensive deception methods aim to confuse an attacker and accomplish attack failure. Nevertheless, the majority of defensive deception strategies in game theory are predicated on the idea that individuals maintain consistent viewpoints when faced with ambiguity. They disregard the fact that participants may have subjective views based on information that is unequally distributed. In this paper, we design a hypergame in which an attacker and a defense may both take a belief-based approach to the same game and choose the optimal strategy. The belief of the attackeris crucial to their decision-making process, and defensive deception methods may alter this belief. Here we take advanced persistent threat (APT) assaults into account; they include a series of assaults carried out at different points in the cyber kill chain, with the goal of both the attacker and the defense choosing the best possible strategy according to their views. In a hyper game where the imperfect information is reflected by perceived uncertainty, cost, and expected utilities of both the attacker and the defender, the system lifetime (i.e., mean time to security failure), and improved false positive rates in detecting attackers, we showed through extensive simulation experiments how the defender can effectively use defensive deception techniques while dealing with multi-staged APT attacks.

Keywords: Using Hyper game Theory for Defensive Deception Against Advanced Persistent Threats: Four Eye.

INTRODUCTION:

Tricking an attacker into doing a less-than-ideal action that will lead to the failure of an assault is the main goal of defensive deception techniques. Strategic exchanges may be crucial for victory when both sides are strapped for resources. As a result of not having access to efficient and successful strategic strategies, non-game-theoretic defense measures have limits too. Many different

Corresponding Author e-mail: : ramanmass01@gmail.com
How to cite this article: 1DR. M. RAMASUBRAMANIAN, 2SUNKARA SHREE SHREYA, 3KUMMARI BHAVANA, 4AKINA DIVYA. Using Hyper game Theory for Defensive Deception Against Advanced Persistent Threats: Four Eye.Pegem Journal of Education and Instruction, Vol. 13, No. 3, 2023, 489-503
Source of support: Nil **Conflicts of Interest:** None.
DOI: 10.47750/pegegog.13.03.49
Received: 12.09.2023
Accepted: 22.10.2023 **Published:** 24.11.2023

kinds of deceitful tactics have been considered according to specific categories, such as shielding the work of Jin-He Cho and Zelin Wan was supported by the Department of Computer Science at

Virginia Tech in Falls Church, VA 22043, USA. The email address is {Zalin, Jiho}@vt.edu. They are Mu Zhu and Munindra P. Singh from the Computer Science Department of North Carolina State University in Raleigh, NC 27695, USA. Electronic mail: {mzhu5, musing}@ncsu.edu. In Adelphi, Maryland, USA, Ahmed H. Anwar and Charles A. Kahlua are affiliated with the US Army Research Laboratory. Two email addresses: a.h.anwar@knights.ucf.edu

and charles.a.kamhoua.civ@mail.mil.
authenticity vs. spreading misinformation, or passive vs. aggressive to make the attackers more confused or ambiguous.
Under the assumption that participants have consistent opinions, game theory has found extensive application in the context of uncertain, dynamic decision-making. Due to the fact that participants may often subjectively analyze information that is asymmetrically accessible to them, this premise is false. One subfield of game theory, known as "hyper game theory," offers an analytical framework that takes into account the impact of subjective factors like belief, misbelief, and perceived uncertainty on strategy choice. Using hyper game theory as a strong decision-making mechanism in uncertain situations, this study may settle conflicts of views among several participants, even if they have diverse ideas about the same game. In order to counter APT assaults, hyper game theory simulates participants, including cyber attackers and defenders. This Endeavour is dubbed Four Eye after the Four Eye butter flyfish, which exemplifies a deceitful defensive strategy in nature. With precision, we pinpoint the following nontrivial obstacles to finding a solution. Deriving realistic game situations and developing defensive deception strategies to cope with APT assaults beyond the reconnaissance stage is not straightforward. The current state of the art has not addressed this angle. For another, it's not easy to put a number on how much room for

error there is in the perspectives of both attackers and defenders; nonetheless, these perspectives are crucial, since the way each side perceives the game greatly influences the tactics it employs. Third, in adversarial settings, it is expensive to deploy and maintain defensive deception tactics, and dealing with a large number of solution spaces is not straightforward when there are many options under dynamic scenarios. While our earlier work did some work on these issues, it only covered a small-scale network and a handful of methods using a Stochastic Petri Net-based, very simplified probability model, so it didn't help much overall. Particularly noteworthy are the following new contributions to the field that this work introduces: Using hyper game theory, we simulated an attack-defense game in which both players are unaware of the other's strategy and have divergent perspectives on the current position. • A player's belief in the face of uncertainty is used to design each subgame in the cyber kill chain (CKC), which in turn reduces the player's action space by adopting one of the possible methods. • In our analysis, we took into account a variety of defensive methods, including defensive deception techniques. The effectiveness of these approaches may be influenced by the attacker's beliefs and perceived uncertainty, which in turn influence their strategy choice. Based on the amount of time each player has spent observing the opponent and their plan, we were able to simulate the attacker's and defender's doubt about their opponent. As far as we are aware, previous studies on hyper game theory have specified a constant probability to stand in for a player's uncertainty. In this study, we calculated the player's uncertainty by modeling the evolving strategic exchanges between the offence and defense. • We compared abilities both with and without an attacker using defending deception (DD) tactics, as well as with and without complete insight into the opponent's moves. The perceived insecurity, hyper game expected utility, action cost, mean time until security failure (MTTSF or system lifetime), and increased false positive rate (FPR) of an intrusion detection using DD strategies utilized by the defender were some of the metrics used to measure the efficacy and efficiency of DD techniques in relation to the security and performance of a system.

Related Work:

A More Efficient Between’s Centrality Algorithm

This study introduces novel techniques for between’s, which are driven by the rapidly increasing need to calculate centrality indices on massive networks that are very sparse. On unweighted networks, they take O(nm) time and $O(nm + n^2 \log n)$ space, whereas on weighted networks, they take

O(nm + m) time, with m being the number of connections. This widens the scope of networks that may be included for centrality analysis, according to the experimental findings. Although it is vital for social network research, computing the between's centrality index may be expensive. At now, the most efficient techniques in the field necessitate? (n ^{3}) time and? (n ^{2}) space, where n is the numerical value of the network's actors.

A First-Level Hypergame for Studying Conflict Misunderstandings

Within the context of the graph model for conflict resolution, a novel approach is presented to represent the possibility of misunderstandings among the decision makers (DMs) involved in a dispute involving several DMs. Using this all-encompassing method, one may simulate a conflict scenario where there is misunderstanding, both on the part of the central DM and its opponents. Specifically, this is accomplished by categorizing the available choices to DMs in a conflict scenario according to the many forms of misperception that might influence the decisions made by the focal DM and/or the other DMs. In addition, the universal set of states may be constructed from the combination of the alternatives given by the DMs during the whole war. With this innovative layout, we can tell which states are universally recognized and which ones are recognized specifically by DMs. Additionally, eight sets of equilibrium are explicitly described inside the first-level hyper game's graph construction to represent the impact of DMs' misunderstandings on the dispute's equilibrium and to provide strategic insights into the conflict.

Cyber security fraud

Imagine two enemies going head-to-head, each with similar skills but different objectives. Tossing a coin typically determines the likelihood of their winning. How about if one of them could take use of targeted data, adaptability, and speed? There's no fight. Competitors that are quicker and more agile tend to come out on top. But the latter is stronger and has more knowledge at their fingertips. Why? Since the better-informed opponent eventually succumbs to "analysis paralysis." They have amassed an enormous amount of data, making it impossible to analyze everything without prioritizing certain details. In a fight, this is how the weaker opponent often emerges victorious.

Hypergamies for Cyber-Physical Security: Learning and Information Manipulation

Cyber-attacks on cyber-physical systems may have devastating real-world effects. Our earlier research demonstrated the feasibility of using hyper game analysis—a generalization of game theory to scenarios including information asymmetries and player misperceptions—to control systems vulnerable to assaults based on deceit. We expand upon that work by investigating a recurrent stochastic setting here. We think about the possibility of detecting an unseen attacker trying to control the system. We outline a learning plan for the defender and talk about several monitoring mechanisms that might be utilized for this purpose. Our numerical studies show that the cost of defending against an attacker has a significant effect on both the impact of the attacker and the time it takes to identify them. Further, we demonstrate that the defender learning scheme causes the attacker to make a tough choice between being identified and making an influence on the system.

In the direction of a hypergame theory

The stability perspective is used to study differential games (DGs). There are a number of parallels between structural stability theory and optimal control theory that point to a differential game approach, where operators' conflicts of interest are limited to the system's stability. This qualitative method brings a number of novel and intriguing aspects. The differential hyper game (DHG) is the equilibrium position of a dynamical system within the context of a certain stability theory; it is the solution of a differential game. We cover three varieties of DHG: abstract structural, Lyapunov, and Popov. The first one establishes a link between DG and Thom's catastrophe theory; the second one relates the value function method to Lyapunov theory; and the third one gives DG specific, invariant characteristics. The current issue with the global economy is described to show that the proposed theory could have intriguing uses. **Botnets and the safety of the Internet of Things**

The recent spate of distributed denial-of- service attacks highlights how susceptible IoT systems and devices are. Scalable security solutions that are tailor-made for the Internet of Things (IoT) ecosystem are essential for tackling this problem.

METHODOLOGY:

As a first line of defense, an attacker may use a monitoring attack to identify vulnerable nodes in a network and launch an assault on them.

Approach to Attack AS2: Social Engineering, in which an attacker sends phishing emails including URL links; if the target clicks on the links, malicious software is installed, and the attackers get sensitive information such as passwords and cookies.

Approach to Attack Method 3 (AS3): Botnet, which infects all nodes in a network with malware. Attack Type 4: Distributed Denial of Service Attacks in Which the

Attacker Sends a Deluge of Requests to the Target Server in an Effort to Crash It.

Method of Attack 5: A zero-day attack may take advantage of unpatched software vulnerabilities.

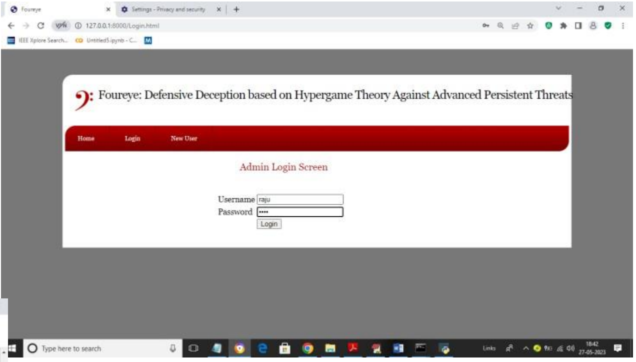
Method Six: Cracking Encryption: One example is the compromising of a legal node's private or secret key. The intruder in possession of the encryption key is regarded as an insider threat as they have the ability to abuse system resources. The author has offered six potential responses to the aforementioned threats.

1) Fix (DS1): Installing firewalls is essential for preventing vulnerabilities.
2) Solution (DS2): Patch Management, which involves deploying fixes for all potential vulnerabilities that may be detected in assaults.
3) (DS3) The creation of new encryption keys, often known as cryptography. By constantly generating new keys, this method will make it more difficult for attackers to guess them. To prevent attacks, we need to implement the rekeys procedure.
4) Fix (DS4): Eliminating all traces of past assaults and attackers is essential.
Option 5 (DS5): Minimal and Maximum Interaction It is necessary to set up honey pots.
6) DS6 Solution: A honeypot records all users' login information. If a user repeatedly enters incorrect details in an attempt to

guess a password, the honeypot will send false information to the attacker, leading him to believe that he has invaded the network. In response, the honeypot will collect all of the data the attacker has requested and restrict his access.

RESULTS:

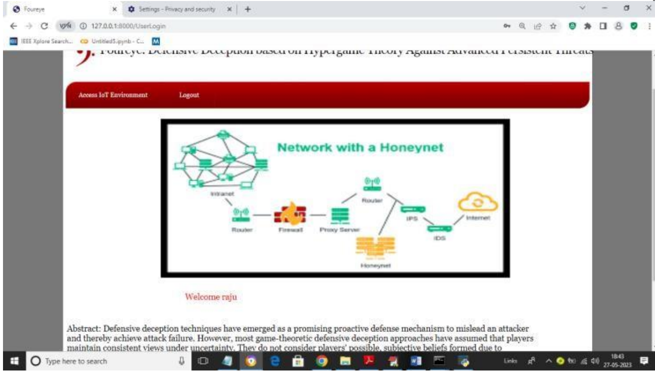
If Honeypot identifies the user "raju" as an attacker on the previous screen, it will block access to the server on the next page.



Foureye: Defensive Deception based on Hypergame Theory Against Advanced Persistent Threats

Admin Login Screen

Username raju
Password ••••

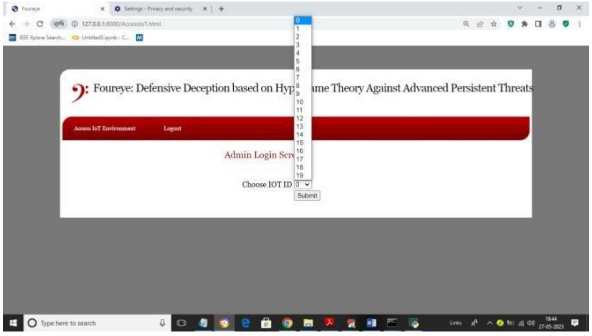


Foureye: Defensive Deception based on Hypergame Theory Against Advanced Persistent Threats

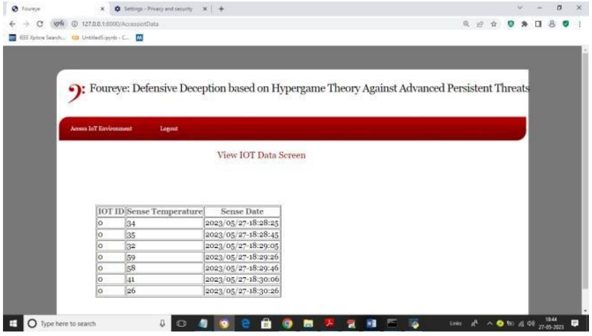
Welcome raju

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

In addition to the preceding panel, the attacker may access the following page by clicking the link labeled "Access IOT Environment."



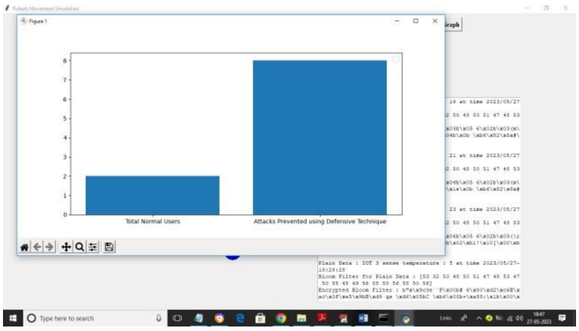
By clicking the Submit button on the previous panel, the attacker may access the next page after setting the IOT ID to 0.


Foureye
Settings - Privacy and security
127.0.0.1:8000/AccessIotData
IEEE Xplore Search...
Untitled5.ipynb - C...
Foureye: Defensive Deception based on Hypergame Theory Against Advanced Persistent Threats
Access IoT Environment
Logout
Type here to search
Links
18:44
27-05-2023

View IOT Data Screen

IOT ID	Sense Temperature	Sense Date
0	34	2023/05/27-18:28:25
0	35	2023/05/27-18:28:45
0	32	2023/05/27-18:29:05
0	59	2023/05/27-18:29:26
0	58	2023/05/27-18:29:46
0	41	2023/05/27-18:30:06
0	26	2023/05/27-18:30:26

Since the actual temperature sensed by the IOT at row 1 is 16, the attacker may observe that the displayed value is 34 on the above screen. We may thwart attackers and keep them at bay by using deceitful techniques. To access the section below on attack detection and prevention, go to the simulation screen and click on the "Vulnerability Detected Comparison Graph" button.



```
Plain Data : IOT 3 sense temperature : 5 at time 2023/05/27-
18:28:28
Bloom Filter for Plain Data : [53 32 50 48 50 51 47 48 53 47
 50 55 45 49 56 58 50 56 58 50 56]
```

The graph above shows the total number of attackers discovered and stopped, the total number of legitimate users who logged in, and the number of people who logged in on the x-axis.

You may also access IOT data, log in, and create an account by following the steps outlined above.

CONCLUSION

We derived the following important conclusions from this study: Defense by deception (DD) is a strategy for reducing the perceived uncertainty of both the attacker and the defense. This is due to the fact that an insider hacker gains a false sense of security as it gains access to more sensitive system information. Hyper game expected utilities (HEUs) are determined, among other things, by the attack cost and the defense cost. On the flip side, defenders may minimize their uncertainty by gathering more attack information via DD while still letting attackers into the system. Thus, although a high DHEU (defender's HEU) is impressive, it does not guarantee a high MTTSF (mean time to security failure) or TPR (true positive rate), two important metrics for system security. This means that out of all the schemes, DD under imperfect information (IPI) produces the shortest DHEU and the highest performance in MTTSF (the longest system lifespan). The DD techniques may successfully raise the TPR of the system's NIDS by using the attack information they acquire. This work raises important questions that need answering in the following ways: (1) how to account for simultaneous attacks on a system for more realistic scenarios; (2) how to use machine learning to estimate each player's beliefs for better opponent prediction; (3) how to dynamically adjust a risk threshold based on the security state of the system; (4) how to restore a compromised node to a healthy one while allowing for recovery delay; (5) how to create an intrusion response system that can reassess detected intrusions to minimize false positives while identifying an optimal response strategy to handle high-priority intrusions; and (6) what about another intrusion prevention mechanism.

REFERENCES

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

[2] Y. M. Allegri, M. A. Bashar, L. Fang, and k. W. Happel, “First-level hyper game for investigating misperception in conflicts,” IEEE Trans. Systems, Man, and Cybernetics: Systems, vol. 48, no. 12, pp. 2158–2175, 2017.

[3] H. Aleska 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: Repeated hypergamic for cyber-physical security,” IEEE Control Systems Letters, vol. 4, no. 2, pp. 295–300, 2019.

[5] P. G. Bennett, “Toward a theory of hyper games,” Omega, vol. 5, no. 6, pp. 749–751, 1977.

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

[7] M. Brossard, D. T. Bui, L. Ciavaglia, R. Douville, M. L. Palac, N. L. Suze, L. Nouria, S. Papillon, P. Peloso, and F. Santoro, “Software-defined LANs for interconnected smart environment,” in 2015 27th Int’l Tele traffic Congress, 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 investigation of deception in network security,” Security and Communication Networks, vol. 4, no. 10, pp. 1162–1172, 2011.

[11] W. Casey, A. Kellner, P. Mimarmosher, J. A. Morales, and B. Mishra, “Deception, identity, and security: The game 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 and Analysis of Deception

Games based on hypergamic 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 of Security. ACM, 2019, p. 4.

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

[15] N. Garg and D. Grosu, “Deception in honeynets: A game-theoretic analysis,” in Proc. IEEE Information Assurance and Security Workshop (IAW). IEEE, 2007, pp. 107–113.

[16] B. Harsimar and J. Cortes, “Evolution of the percept- ´ Tion about the opponent in hyper games,” in Proc. 49th IEEE Conf. Decision and Control (CDC), Dec. 2010, pp. 1076–1081.

[17] ——, “Evolution of players’ misperceptions in hyper games under perfect observations,” IEEE Trans. Automatic Control, vol. 57, no. 7, pp. 1627–1640, Jul. 2012.

[18] I. GmbH. Mind Node. [Online]. Available: https: //mindnode.com/

[19] J. Han, J. Pei, and M. Kamber, Data Mining: Concepts and Techniques. Elsevier, 2011.

[20] J. T. House and G. Benko, “hypergamic theory applied to cyber-attack and defense,” in Proc. SPIE Conf. Sensors,

and Command, Control, Comms., and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense IX, vol. 766604, May. 2010.

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

[22] N. S. Kovach, A. S. Gibson, and G. B. Lamont, "hypergamic theory: A model for conflict, misperception, and deception," Game Theory, 2015, article ID 570639, 20 pages.

[23] K. Krummholz, H. Hobel, M. Huber, and E. Weippe, "Advanced social engineering attacks," Jour. Information Security and Applications, vol. 22, pp. 113– 122, 2015.

[24] S. Kyung, W. Han, N. Tiwari, V. H. Dixit, L. Srinivas, Z. Zhao, A. Doupe, and

G. Ahn, "Honey proxy: Design ′ and implementation of next-generation honeynet via SDN," in 2017 IEEE Conf. Comms. and Network Security (CNS), Oct. 2017, pp. 1–9.

[25] O. Leiba, Y. Yitzchak, R. Bitton, A. Nadler, and A. Shabtai, "Incentivized delivery network of IoT software up11 dates based on trustless proof-of- distribution," in 2018 IEEE European Symp. on Security and Privacy Workshops (Euro's PW), Apr. 2018, pp. 29–39.

[26] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "SDN-based data transfer security for Internet of Things," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 257–268, Feb. 2018.

[27] D. F. Macedo, D. Guedes, L. F. M. Vieira, M. A. M. Vieira, and M. Nogueira, "Programmable networks—from software-defined radio to software defined networking," IEEE Comms. Surveys Tutorials, vol. 17, no. 2, pp. 1102–1125, Second Quarter 2015.

[28] M. E. J. Newman, Networks: An introduction, 1st ed. Oxford University Press, 2010.

[29] H. Obhrai, M. A. Rabe, W. G. Leonard, T. R. Hobson, D. Bigelow, and W. W. Streilein, "Survey of cyber moving targets," Lexington Lincoln Lab, MIT, TR 1166, 2013.

[30] U. S. Potro, K. Kijima, and S. Takahashi, "Adaptive learning of hyper game situations using a genetic algorithm," IEEE Trans. Systems, Man, and Cybernetics-Part A: Systems and Humans, vol. 30, no. 5, pp. 562–572, Sep. 2000.

[31] Y. Sasaki, "Subjective rationalizability in hyper games," Advances in Decision Sciences, vol. 2014, no. Article ID 263615, p. 7 pages, 2014.

[32] A. Schlenker, O. Thakoor, h. Xu, F. Fang, M. Tambe, L. Tran-Thanh, P. Vaiano's, and Y. Soloveitchik, "Deceiving cyber adversaries: A game theoretic

approach," in Proc. 17th Int'l Conf. Autonomous Agents and Multiagent Systems, 2018, pp. 892–900.

[33] W. L. Sharp, "Military deception," Joint War-Fighting Center, Doctrine and Education Group, Norfolk, VA, Pub. 3-13.4, 2006.

[34] S. Tadley's, Game Theory. Princeton University Press, 2013.

[35] Y. W. The, Dirichlet Process. Boston, MA: Springer US, 2010, pp. 280–287.

[36] R. Vane, hypergamic theory for DTGT agents. AAAI, 2000.

[37] ——, "Planning for terrorist-caused emergencies," in Proc. Winter Simulation Conf., Dec. 2005.

[38] ——, "Advances in hyper game theory," in Proc. AAMAS Workshop on Game-Theoretic and Decision Theoretic Agents, 2006.

[39] R. Vane and P. E. Lehner, "Using hyper games to select plans in adversarial environments," in Proc. 1st Workshop on Game Theoretic and Decision Theoretic Agents, 1999, pp. 103–111.

[40] Wikipedia. (2018) Four eye butterflyfish. Available at https://en.wikipedia.org/wiki/Foureye butterflyfish.

[41] Y. Yin, B. An, Y. Vorobey, and J. Zhuang, "Optimal deceptive strategies in security games: A preliminary study," in Proc. AAAI Conf. Artificial Intelligence, 2013.