**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 misperception

in 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: Repeated

hypergames for cyber-physical security,” IEEE

Control 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 Things

security,” 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 interconnected

smart environment,” in 2015 27th Int’l Teletraffic

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. Memarmoshrefi, 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 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 of

Security. ACM, 2019, p. 4.

[14] N. M. Fraser and K. W. Hipel, 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. Gharesifard and J. Cort´es, “Evolution of the perception

about the opponent in hypergames,” in Proc. 49th

IEEE Conf. Decision and Control (CDC), Dec. 2010, pp.

1076–1081.

[17] ——, “Evolution of players’ misperceptions in hypergames

under perfect observations,” IEEE Trans. Automatic

Control, vol. 57, no. 7, pp. 1627–1640, Jul. 2012.

[18] I. GmbH. MindNode. [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. Cybenko, “Hypergame 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 hypergames,” 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, “Hypergame

theory: A model for conflict, misperception,

and deception,” Game Theory, 2015, article ID 570639,

20 pages.

[23] K. Krombholz, H. Hobel, M. Huber, and E. Weippl,

“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. Doup´e, and G. Ahn, “Honeyproxy: 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 up-dates based on trustless proof-of-distribution,” in 2018

IEEE European Symp. on Security and Privacy Workshops

(EuroS PW), Apr. 2018, pp. 29–39.