Towards Creating a New Cybersecurity Game Theory: Gaps and Potential Bridges

Brandon C. Collins, Shouhuai Xu, and Philip N. Brown

Department of Computer Science, University of Colorado Colorado Springs

Why Game Theory For Cybersecurity?

Problem: Cybersecurity is often done *ad hoc* (i.e., Art) and needs more disciplined solutions (i.e., Science)!

Game Theory is a field of mathematics studying rigorous models of interacting decision makers.

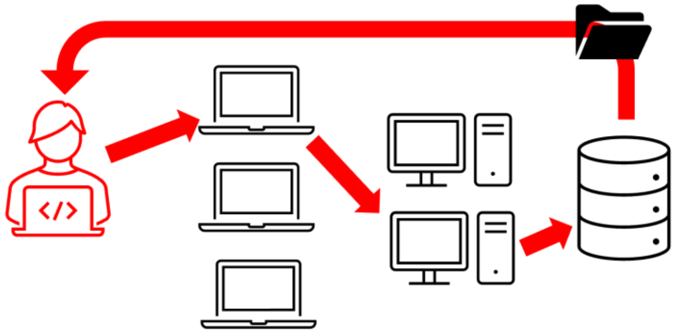
Consider an example:

Attack Successful
Attack Defended
Monitor Nothing
Nothing Happens

😈

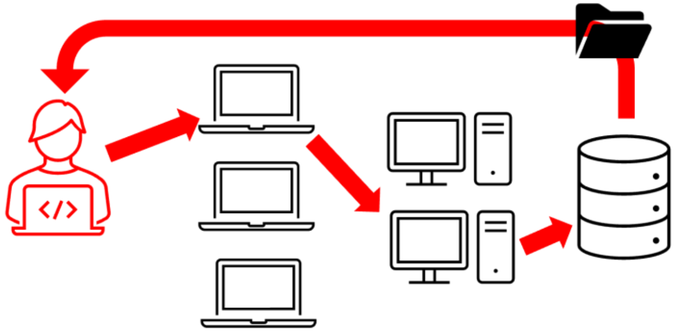
🧠	Attack	Wait
Monitor	**-1,-1**	**-1,0**
Wait	-5,5	0,0

Applications

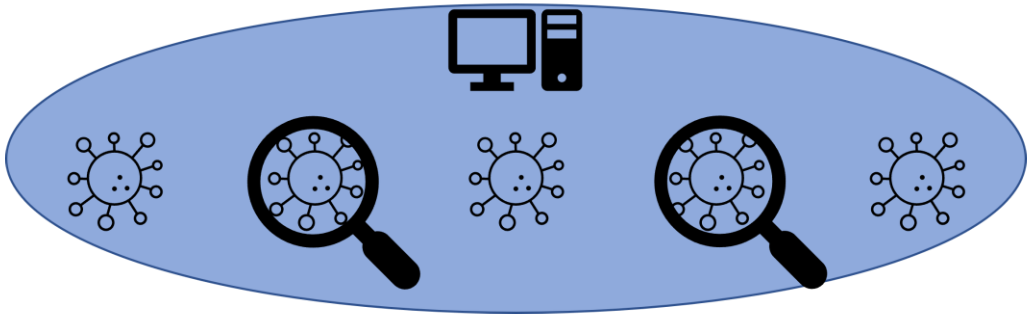


Advanced Persistent Threats

Applications

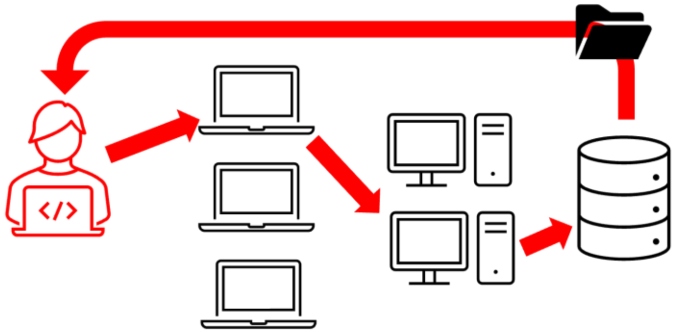


Advanced Persistent Threats

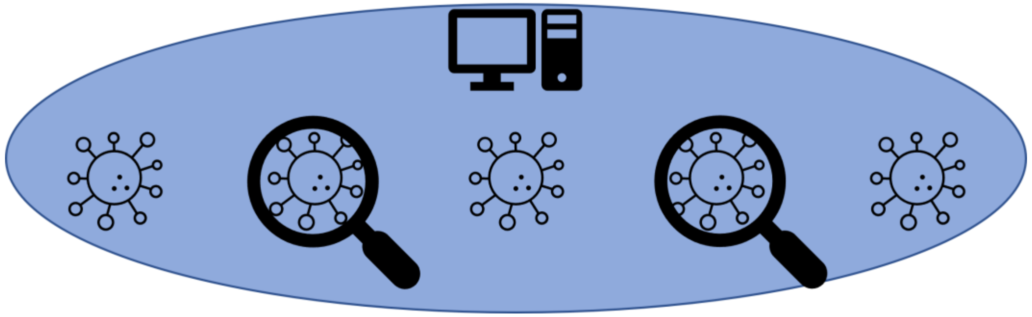


Moving Target Defense

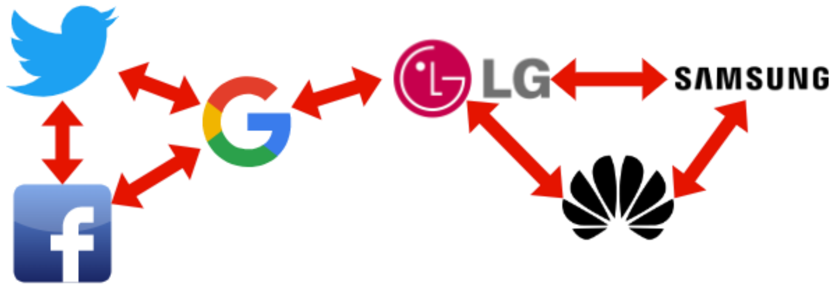
Applications



Advanced Persistent Threats

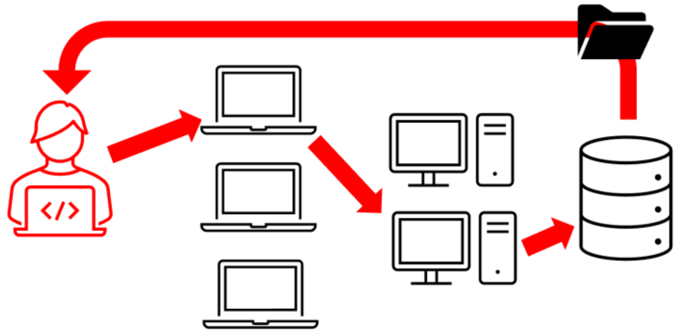


Moving Target Defense

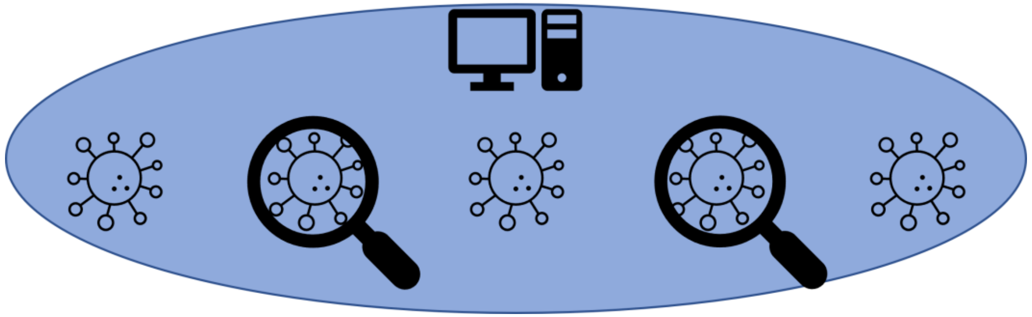


Cyber Threat Intelligence Sharing

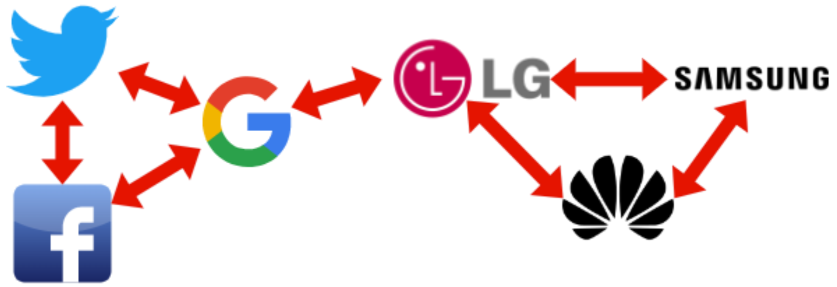
Applications



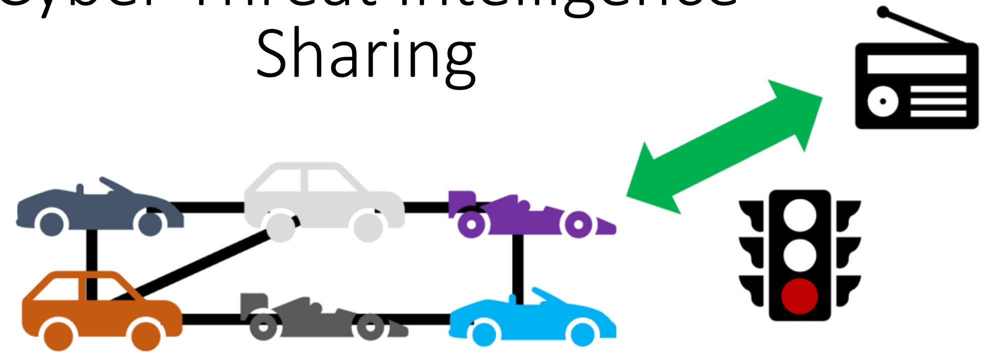
Advanced Persistent Threats



Moving Target Defense

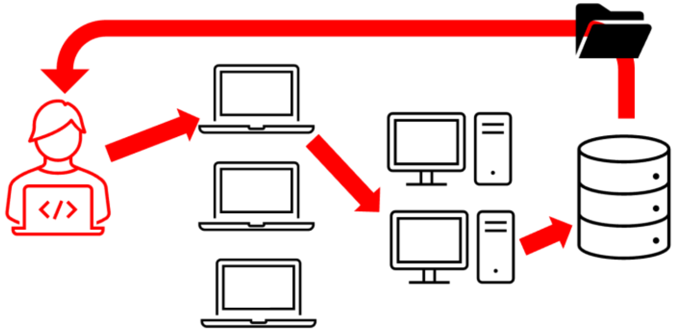


Cyber Threat Intelligence Sharing

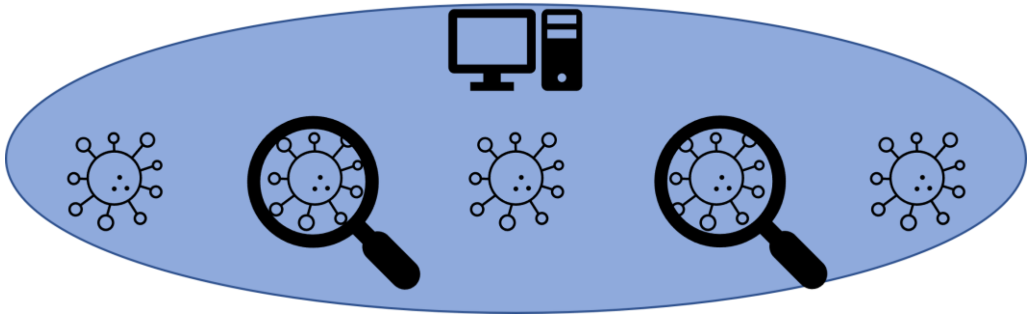


Ad Hoc Networks

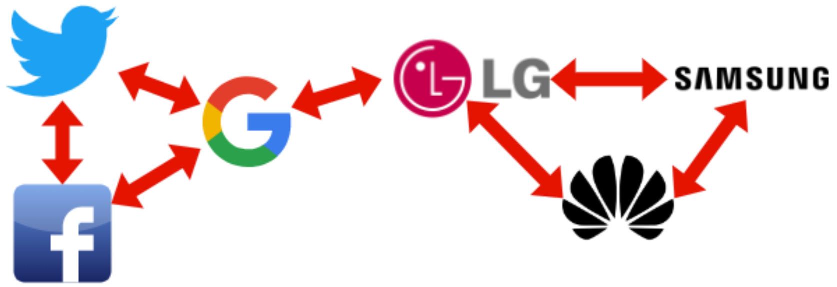
Applications



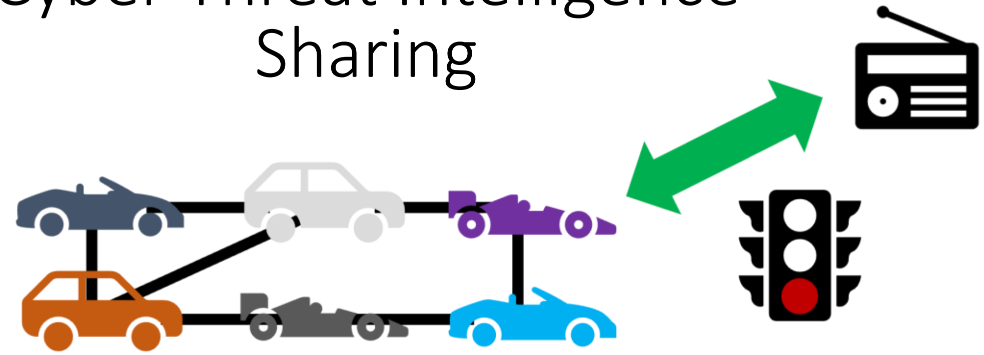
Advanced Persistent Threats



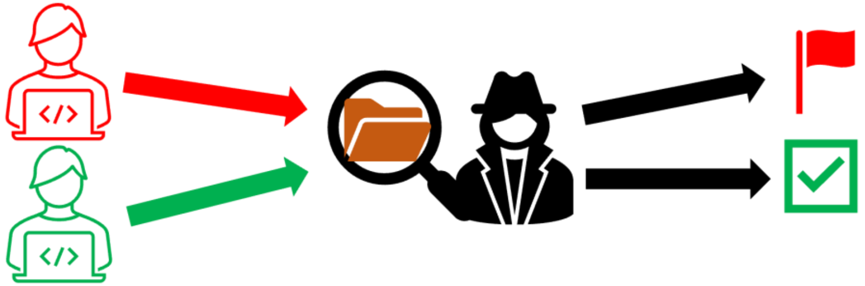
Moving Target Defense



Cyber Threat Intelligence Sharing

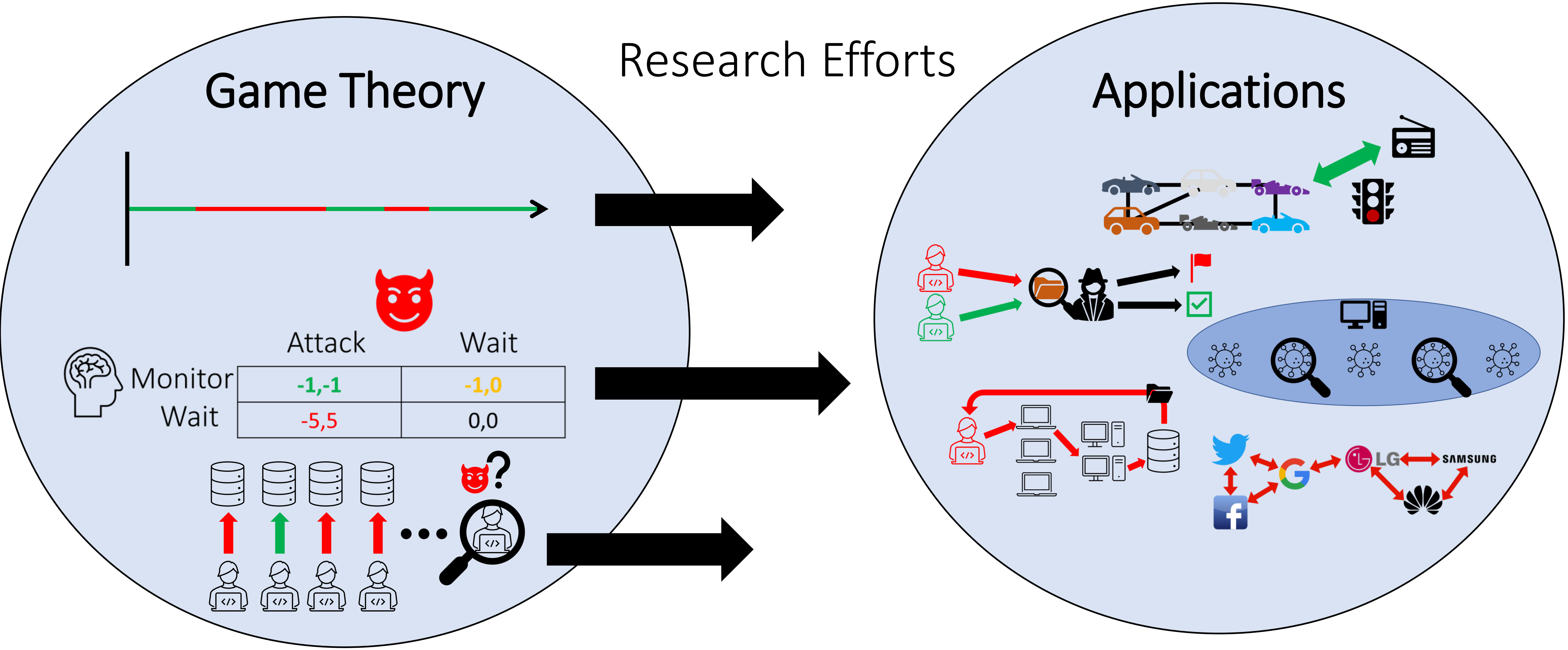


Ad Hoc Networks



Intrusion Detection System Optimization

Our Research



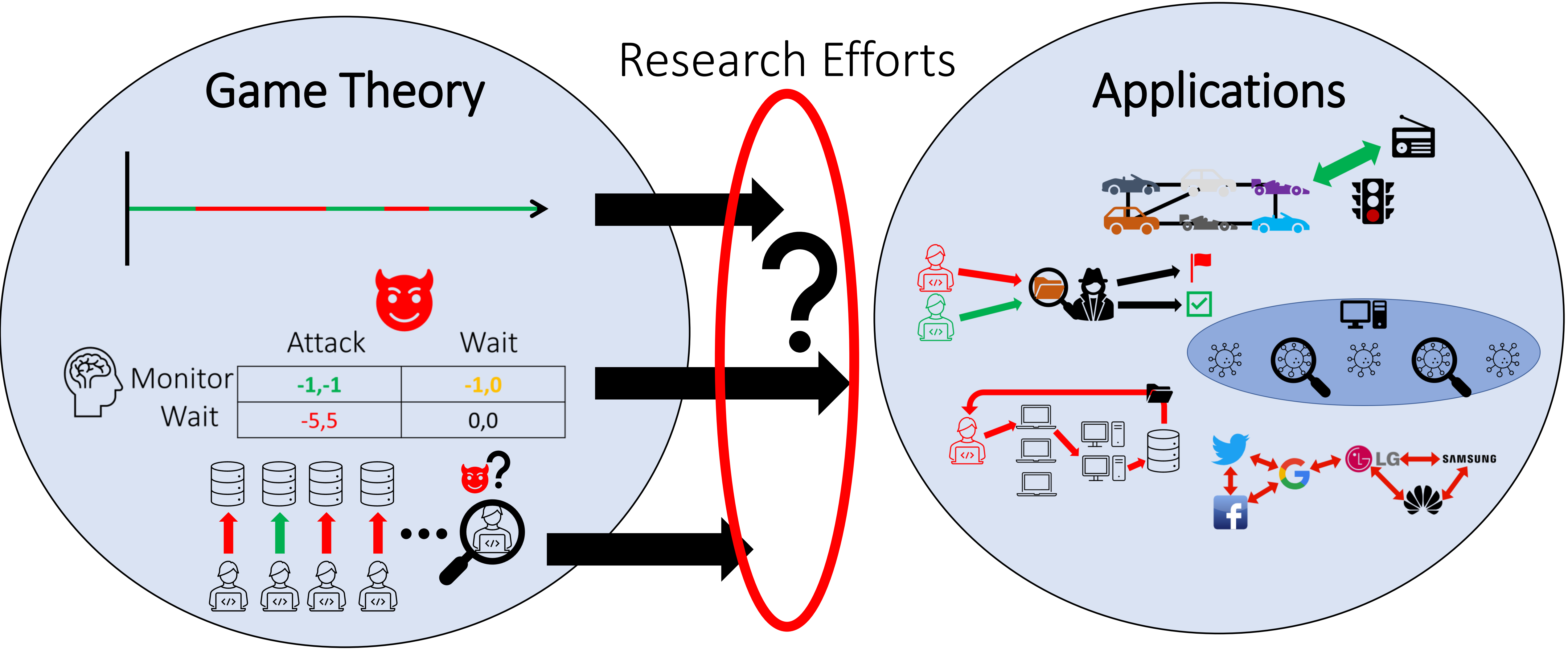
Game Theory

Research Efforts

Applications

	Attack	Wait
Monitor	-1,-1	-1,0
Wait	-5,5	0,0

Our Research



Research Efforts

Game Theory

Applications

	Attack	Wait
Monitor	-1,-1	-1,0
Wait	-5,5	0,0

Q:What is the current state of research?

Models: The Nash Equilibrium

	Attack	Wait
Monitor	**-1,-1**	**-1,0**
Wait	-5,5	0,0

Assumption: Both agents react to each other over time

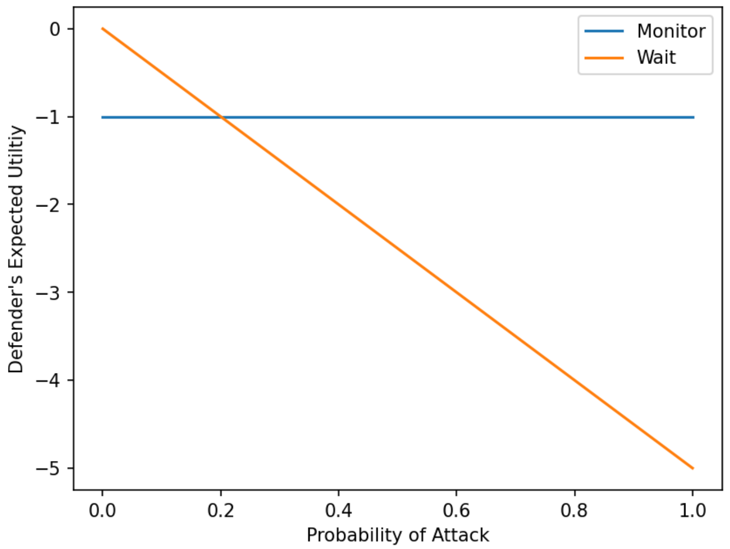
A **Nash Equilibrium** is a joint selection of actions such that no agent can unilaterally improve their utility

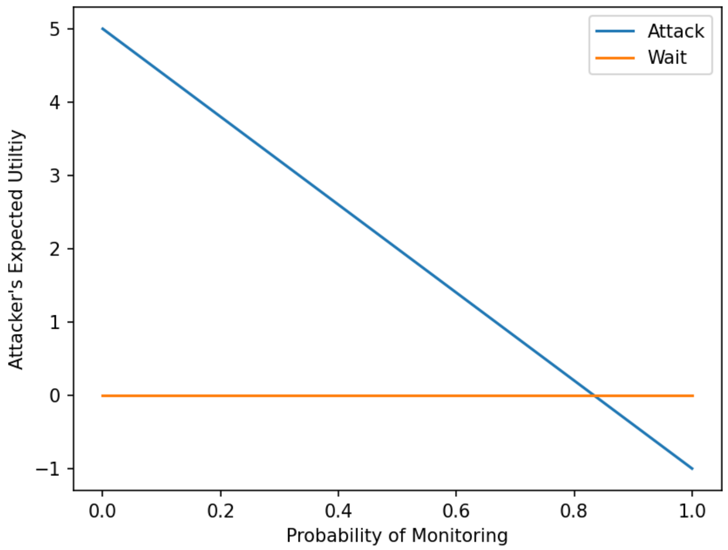
Models: The Nash Equilibrium

	Attack	Wait
Monitor	**-1,-1**	**-1,0**
Wait	-5,5	0,0

Assumption: Both agents react to each other over time

A **Nash Equilibrium** is a joint selection of actions such that no agent can unilaterally improve their utility





Applications

- Advanced Persistent Threats
- Moving Target Defense
- Intrusion detection systems
- Cyberthreat Intelligence Sharing

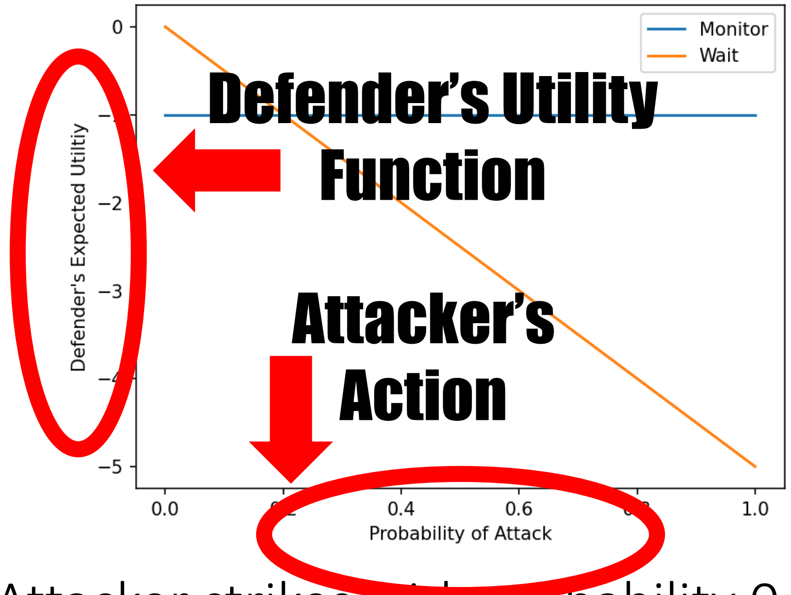
Attacker strikes with probability 0.2! Defender monitors with probability 0.83!

Models: The Nash Equilibrium

	Attack	Wait
Monitor	-1,-1	-1,0
Wait	-5,5	0,0

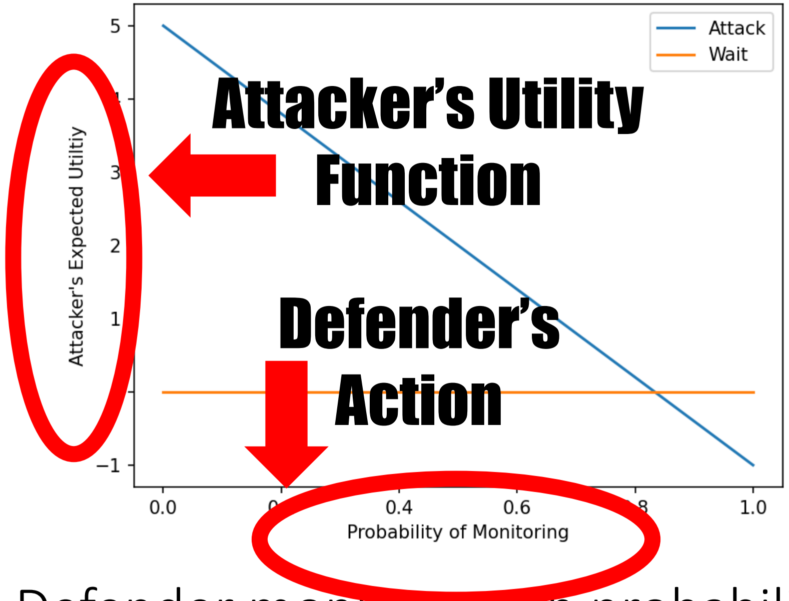
Assumption: Both agents react to each other over time

A **Nash Equilibrium** is a joint selection of actions such that no agent can unilaterally improve their utility



Defender's Utility Function

Attacker's Action



Attacker's Utility Function

Defender's Action

Agents use other agent's perspective to calculate their own action!

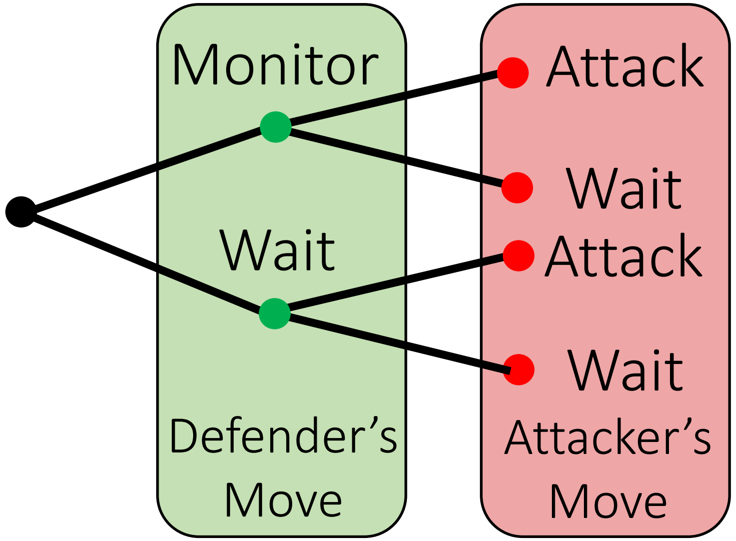
Attacker strikes with probability 0.2! Defender monitors with probability 0.83!

Models: The Stackelberg Equilibrium

	Attack	Wait
Monitor	-1,-1	-1,0
Wait	-5,5	0,0

Assumption: Defender acts first

A **Stackelberg Equilibrium** is a joint selection of actions by a leader and a follower such that no agent can unilaterally improve their utility



Applications

- Moving Target Defense
- Intrusion detection systems

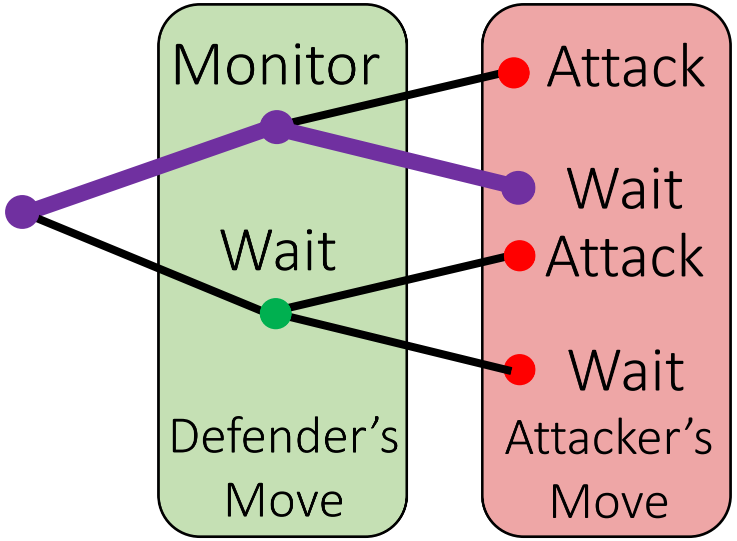
Models: The Stackelberg Equilibrium

	Attack	Wait
Monitor	-1,-1	-1,0
Wait	-5,5	0,0

Assumption: Defender acts first

A **Stackelberg Equilibrium** is a joint selection of actions by a leader and a follower such that no agent can unilaterally improve their utility

Modeling choices impact outcomes!



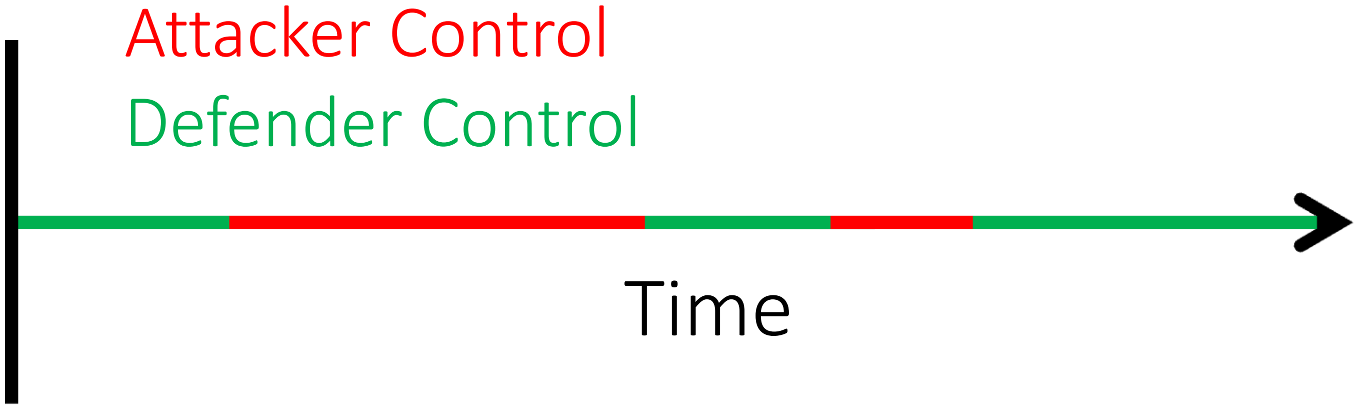
Applications

- Moving Target Defense
- Intrusion detection systems

Defender will always monitor, attacker will never attack!

Models: FlipIt

- Attacker and defender fight for control of a system
- At any time either party may seize control
- Neither know who is currently in control



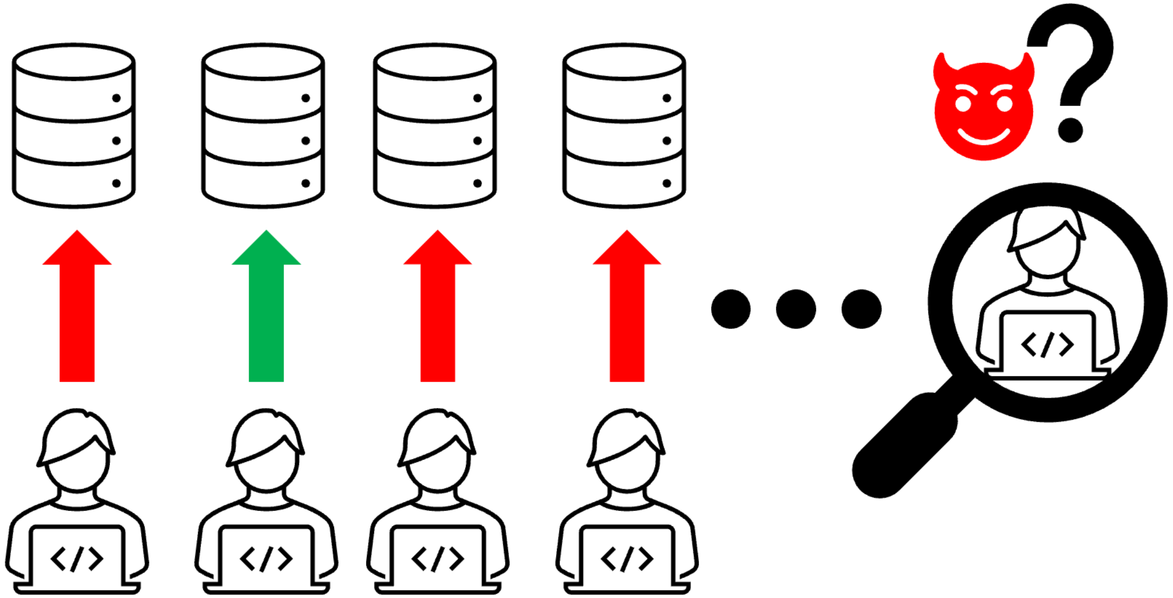
Applications

- Advanced Persistent Threats
- Zero Day Exploits

Q: When should both parties act?

Models: The Bayesian Game

- Agents are unsure of each others' identity
- Each agent maintains a probabilistic belief about other's identities



Applications

- Advanced Persistent Threats
- Moving Target Defense

Q: What is the best course of action given dynamic belief updates?

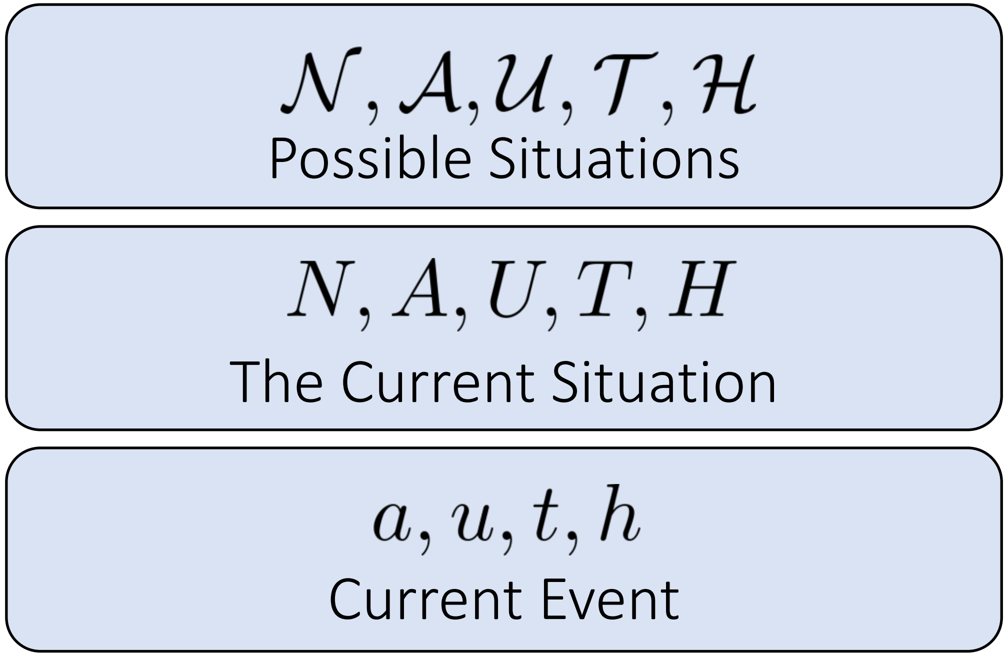
Our Framework

- Models assumptions often implicit
- What information agents have to base decisions on is critical

Our Framework

- Models assumptions often implicit
- What information agents have to base decisions on is critical

Our three-level framework



$\mathcal{N}, \mathcal{A}, \mathcal{U}, \mathcal{T}, \mathcal{H}$

Possible Situations

N, A, U, T, H

The Current Situation

a, u, t, h

Current Event

"What capabilities could they have" $\mathcal{A}$

"How many attackers could there be" $\mathcal{N}$

"What capabilities do they have" A

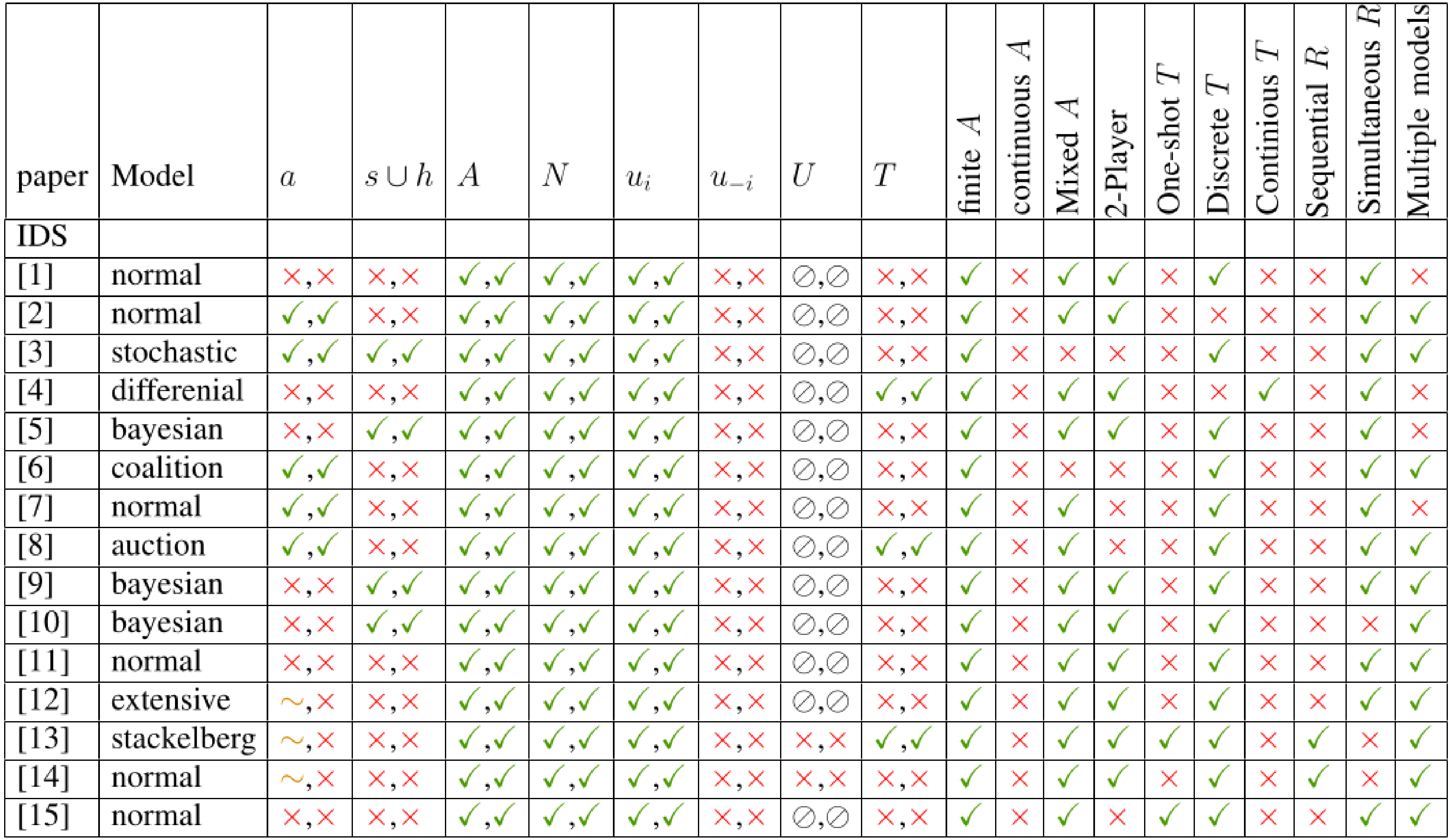
"How many attackers are there" N

"What are they doing right now" a

Key:

N	A	U	T	H
agents	actions	utility	time	history

Findings

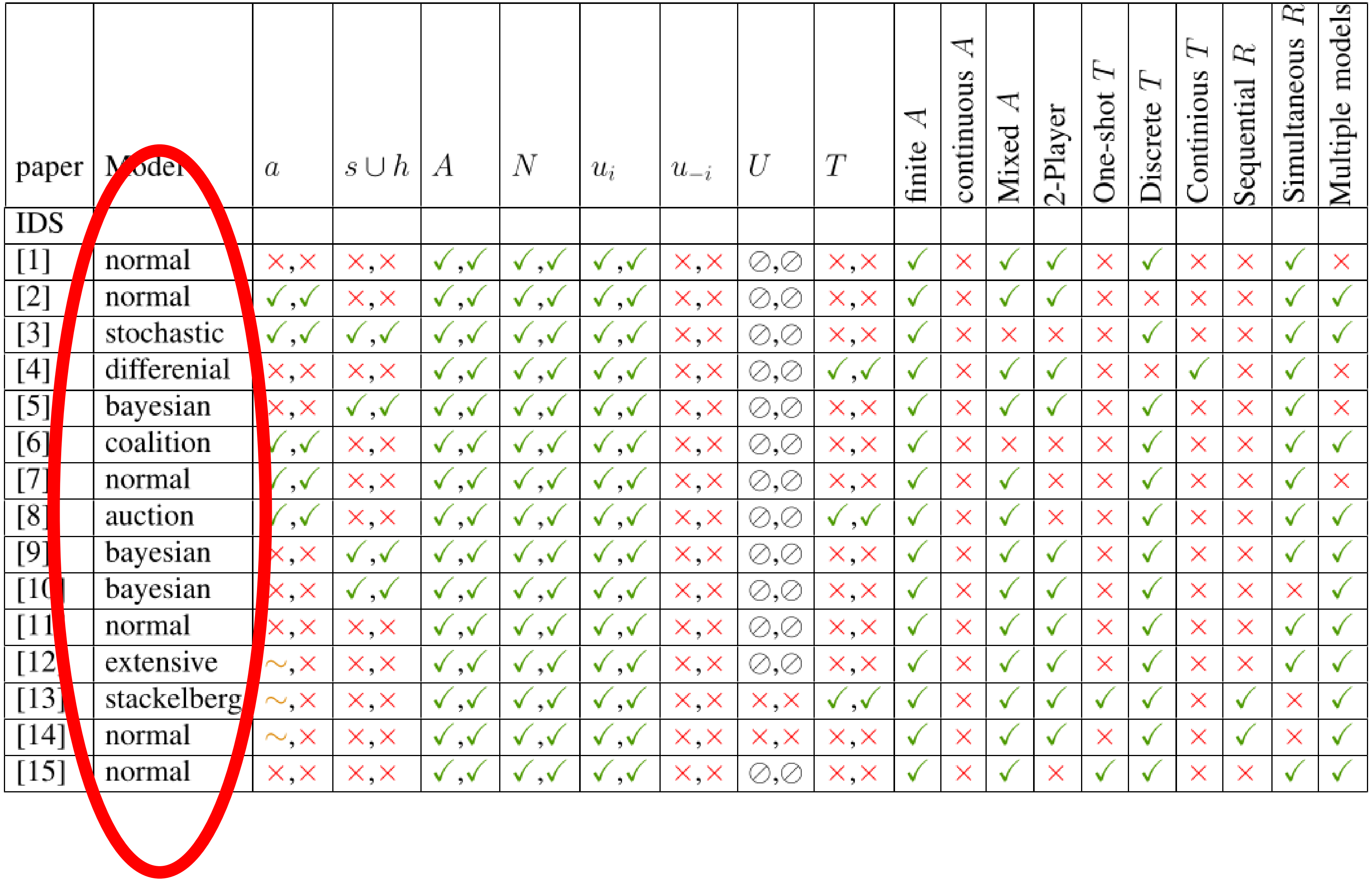


paper	Model	a	$s \cup h$	A	N	u_i	u_{-i}	U	T	finite A	continuous A	Mixed A	2-Player	One-shot T	Discrete T	Continious T	Sequential R	Simultaneous R	Multiple models
IDS																			
[1]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	×
[2]	normal	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	×	×	×	✓	✓
[3]	stochastic	✓,✓	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	×	×	×	✓	×	×	✓	✓
[4]	differenial	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	✓,✓	✓	×	✓	✓	×	×	✓	×	✓	×
[5]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	×
[6]	coalition	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	×	×	×	✓	×	×	✓	✓
[7]	normal	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	×	×	✓	×	×	✓	×
[8]	auction	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	✓,✓	✓	×	✓	×	×	✓	×	×	✓	✓
[9]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[10]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	×	✓
[11]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[12]	extensive	~,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[13]	stackelberg	~,×	×,×	✓,✓	✓,✓	✓,✓	×,×	×,×	✓,✓	✓	×	✓	✓	✓	✓	×	✓	×	✓
[14]	normal	~,×	×,×	✓,✓	✓,✓	✓,✓	×,×	×,×	×,×	✓	×	✓	✓	×	✓	×	✓	×	✓
[15]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	×	✓	✓	×	×	✓	✓

Observations

- Every green checkmark information are assumed to know

Findings

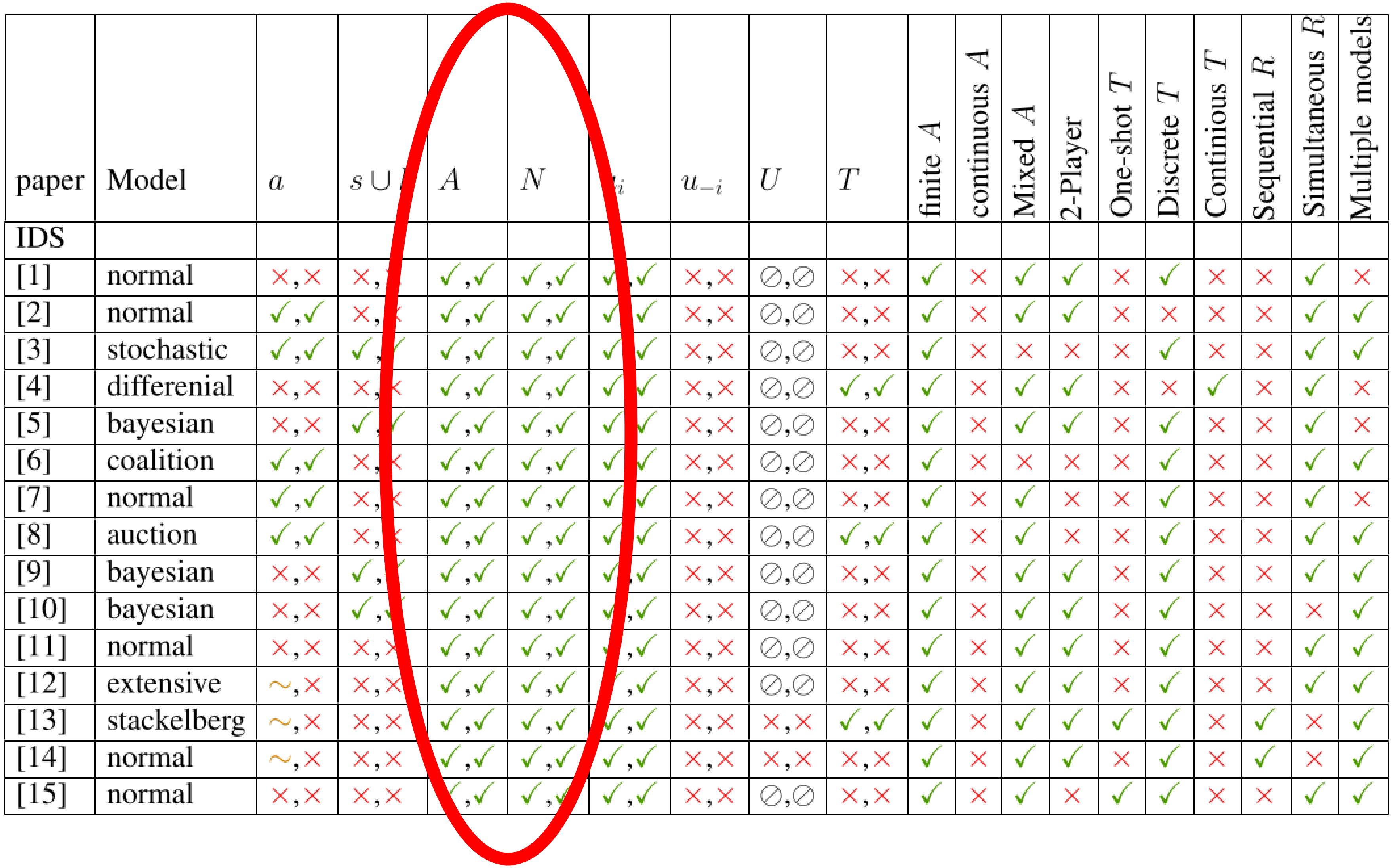


paper	Model	a	$s \cup h$	A	N	u_i	u_{-i}	U	T	finite A	continuous A	Mixed A	2-Player	One-shot T	Discrete T	Continious T	Sequential R	Simultaneous R	Multiple models
IDS																			
[1]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	×
[2]	normal	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	×	×	×	✓	✓
[3]	stochastic	✓,✓	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	×	×	×	✓	×	×	✓	✓
[4]	differenial	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	✓,✓	✓	×	✓	✓	×	×	✓	×	✓	×
[5]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	×
[6]	coalition	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	×	×	×	✓	×	×	✓	✓
[7]	normal	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	×	×	✓	×	×	✓	×
[8]	auction	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	✓,✓	✓	×	✓	×	×	✓	×	×	✓	✓
[9]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[10]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	×	✓
[11]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[12]	extensive	∼,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[13]	stackelberg	∼,×	×,×	✓,✓	✓,✓	✓,✓	×,×	×,×	✓,✓	✓	×	✓	✓	✓	✓	×	✓	×	✓
[14]	normal	∼,×	×,×	✓,✓	✓,✓	✓,✓	×,×	×,×	×,×	✓	×	✓	✓	×	✓	×	✓	×	✓
[15]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	×	✓	✓	×	×	✓	✓

Observations

- Every green checkmark information are assumed to know
- Handful of Game Theoretic Models
- Limited efforts to push them for the needs of cyber security

Findings

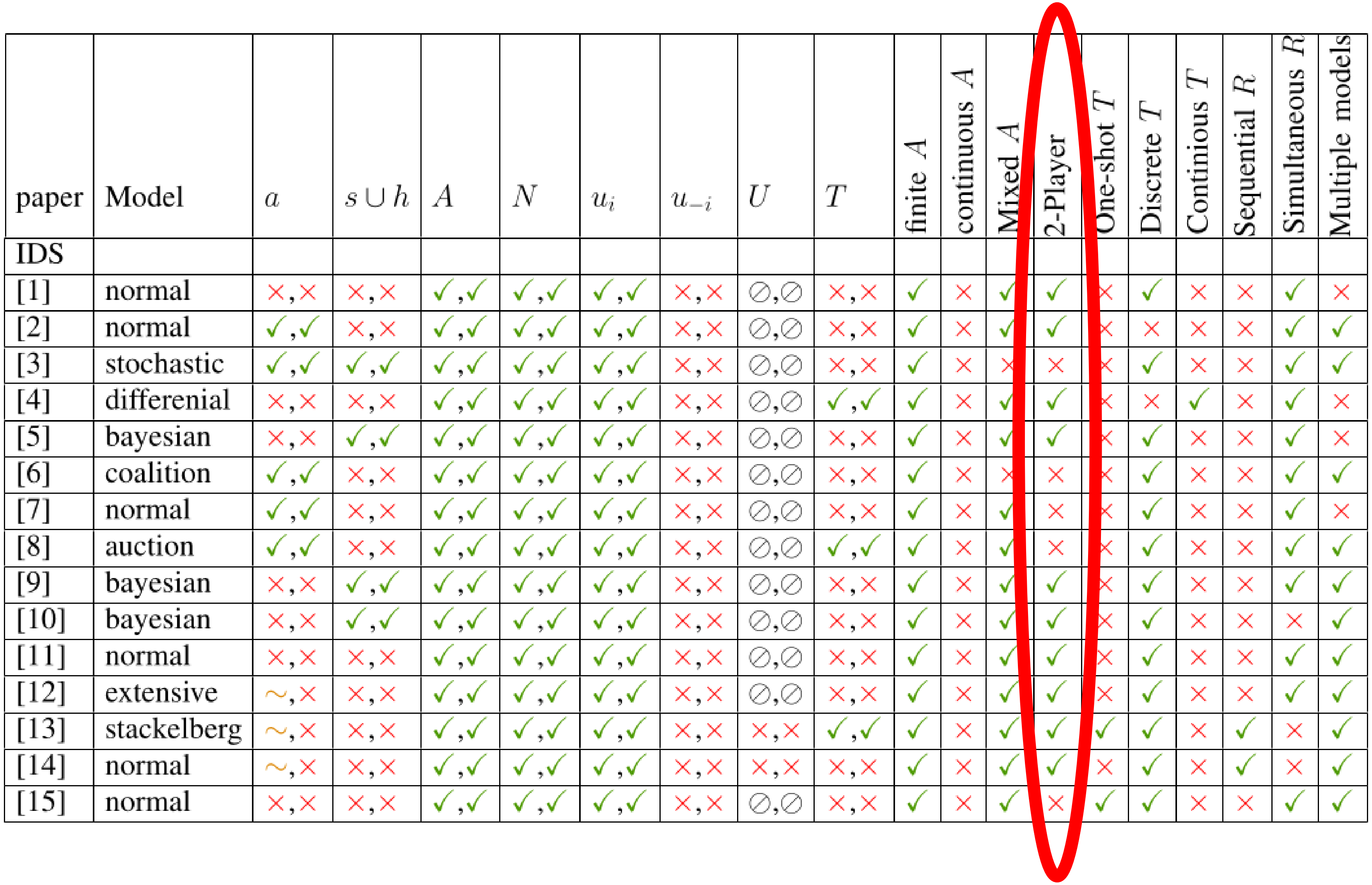


paper	Model	a	$s \cup I$	A	N	u_i	u_{-i}	U	T	finite A	continuous A	Mixed A	2-Player	One-shot T	Discrete T	Continious T	Sequential R	Simultaneous R	Multiple models
IDS																			
[1]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	×
[2]	normal	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	×	×	×	✓	✓
[3]	stochastic	✓,✓	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	×	×	×	✓	×	×	✓	✓
[4]	differenial	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	✓,✓	✓	×	✓	✓	×	×	✓	×	✓	×
[5]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	×
[6]	coalition	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	×	×	×	✓	×	×	✓	✓
[7]	normal	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	×	×	✓	×	×	✓	×
[8]	auction	✓,✓	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	✓,✓	✓	×	✓	×	×	✓	×	×	✓	✓
[9]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[10]	bayesian	×,×	✓,✓	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	×	✓
[11]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[12]	extensive	∼,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	✓	×	✓	×	×	✓	✓
[13]	stackelberg	∼,×	×,×	✓,✓	✓,✓	✓,✓	×,×	×,×	✓,✓	✓	×	✓	✓	✓	✓	×	✓	×	✓
[14]	normal	∼,×	×,×	✓,✓	✓,✓	✓,✓	×,×	×,×	×,×	✓	×	✓	✓	×	✓	×	✓	×	✓
[15]	normal	×,×	×,×	✓,✓	✓,✓	✓,✓	×,×	⊘,⊘	×,×	✓	×	✓	×	✓	✓	×	×	✓	✓

Observations

- Every green checkmark information are assumed to know
- Handful of Game Theoretic Models
- Limited efforts to push them for the needs of cyber security
- Universally assumes agents have precise knowledge of game model

Findings



paper	Model	a	$s \cup h$	A	N	u_i	u_{-i}	U	T	finite A	continuous A	Mixed A	2-Player	One-shot T	Discrete T	Continious T	Sequential R	Simultaneous R	Multiple models
IDS																			
[1]	normal	✗,✗	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✓	✗	✓	✗	✗	✓	✗
[2]	normal	✓,✓	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓
[3]	stochastic	✓,✓	✓,✓	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓
[4]	differenial	✗,✗	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✓,✓	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗
[5]	bayesian	✗,✗	✓,✓	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✓	✗	✓	✗	✗	✓	✗
[6]	coalition	✓,✓	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓
[7]	normal	✓,✓	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✗	✗	✓	✗	✗	✓	✗
[8]	auction	✓,✓	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✓,✓	✓	✗	✓	✗	✗	✓	✗	✗	✓	✓
[9]	bayesian	✗,✗	✓,✓	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓
[10]	bayesian	✗,✗	✓,✓	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✓	✗	✓	✗	✗	✗	✓
[11]	normal	✗,✗	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓
[12]	extensive	~,✗	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓
[13]	stackelberg	~,✗	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	✗,✗	✓,✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✓
[14]	normal	~,✗	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	✗,✗	✗,✗	✓	✗	✓	✓	✗	✓	✗	✓	✗	✓
[15]	normal	✗,✗	✗,✗	✓,✓	✓,✓	✓,✓	✗,✗	⊘,⊘	✗,✗	✓	✗	✓	✗	✓	✓	✗	✗	✓	✓

Observations

- Every green checkmark information are assumed to know
- Handful of Game Theoretic Models
- Limited efforts to push them for the needs of cyber security
- Universally assumes agents have precise knowledge of game model
- Many works only consider 2-agent situation

Metrics

- Agents must measure every green checkmark somehow
- Ad Hoc metrics must go!

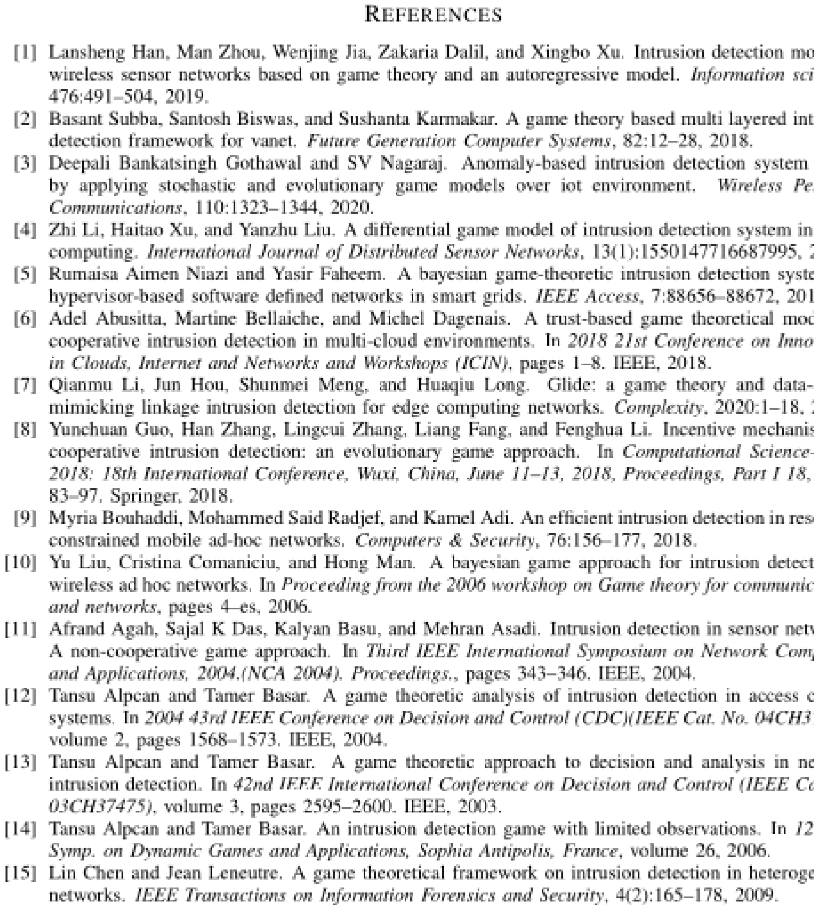
Common Vulnerability Scoring System (CVSS)

- Assigns numeric score to real world exploits describing their severity and ease of use
- Experts use guidelines to qualitatively classify exploits
- CVSS scores leveraged in game theoretics models to understand decision making in the presence of classified exploits!

Conclusion

- Models handle uncertainty in a very limited ways
- Focus on a handful of very well-established models
- Limited work to develop new or push existing models the needs of cybersecurity
- Limited use of metrics to measure needed information

Need to develop new models explicitly for cybersecurity application!



REFERENCES

[1] Lansheng Han, Man Zhou, Wenjing Jia, Zakaria Dalil, and Xingbo Xu. Intrusion detection mo
wireless sensor networks based on game theory and an autoregressive model. *Information sci*
476:491–504, 2019.

[2] Basant Subba, Santosh Biswas, and Sushanta Karmakar. A game theory based multi layered int
detection framework for vanet. *Future Generation Computer Systems*, 82:12–28, 2018.

[3] Deepali Bankatsingh Gothawal and SV Nagaraj. Anomaly-based intrusion detection system
by applying stochastic and evolutionary game models over iot environment. *Wireless Pe*
Communications, 110:1323–1344, 2020.

[4] Zhi Li, Haitao Xu, and Yanzhu Liu. A differential game model of intrusion detection system in
computing. *International Journal of Distributed Sensor Networks*, 13(1):1550147716687995,

[5] Rumaisa Aimen Niazi and Yasir Faheem. A bayesian game-theoretic intrusion detection syste
hypervisor-based software defined networks in smart grids. *IEEE Access*, 7:88656–88672, 201

[6] Adel Abusitta, Martine Bellaiche, and Michel Dagenais. A trust-based game theoretical moc
cooperative intrusion detection in multi-cloud environments. In *2018 21st Conference on Inno*
in Clouds, Internet and Networks and Workshops (ICIN), pages 1–8. IEEE, 2018.

[7] Qianmu Li, Jun Hou, Shunmei Meng, and Huaqiu Long. Glide: a game theory and data-
mimicking linkage intrusion detection for edge computing networks. *Complexity*, 2020:1–18,

[8] Yunchuan Guo, Han Zhang, Lingcui Zhang, Liang Fang, and Fenghua Li. Incentive mechanis
cooperative intrusion detection: an evolutionary game approach. In *Computational Science-*
2018: 18th International Conference, Wuxi, China, June 11–13, 2018, Proceedings, Part I 18,
83–97. Springer, 2018.

[9] Myria Bouhaddi, Mohammed Said Radjef, and Kamel Adi. An efficient intrusion detection in res
constrained mobile ad-hoc networks. *Computers & Security*, 76:156–177, 2018.

[10] Yu Liu, Cristina Comaniciu, and Hong Man. A bayesian game approach for intrusion detect
wireless ad hoc networks. In *Proceeding from the 2006 workshop on Game theory for communic*
and networks, pages 4–es, 2006.

[11] Afrand Agah, Sajal K Das, Kalyan Basu, and Mehran Asadi. Intrusion detection in sensor netv
A non-cooperative game approach. In *Third IEEE International Symposium on Network Com*
and Applications, 2004.(NCA 2004). Proceedings., pages 343–346. IEEE, 2004.

[12] Tansu Alpcan and Tamer Basar. A game theoretic analysis of intrusion detection in access c
systems. In *2004 43rd IEEE Conference on Decision and Control (CDC)(IEEE Cat. No. 04CH3*
volume 2, pages 1568–1573. IEEE, 2004.

[13] Tansu Alpcan and Tamer Basar. A game theoretic approach to decision and analysis in ne
intrusion detection. In *42nd IEEE International Conference on Decision and Control (IEEE Ca*
03CH37475), volume 3, pages 2595–2600. IEEE, 2003.

[14] Tansu Alpcan and Tamer Basar. An intrusion detection game with limited observations. In *12*
Symp. on Dynamic Games and Applications, Sophia Antipolis, France, volume 26, 2006.

[15] Lin Chen and Jean Leneutre. A game theoretical framework on intrusion detection in heteroge
networks. *IEEE Transactions on Information Forensics and Security*, 4(2):165–178, 2009.

Acknowledgement. NSF Grants #2122631, #2115134, and ECCS-#2013779, and Colorado State Bill 18-086.