**Chap 5**

**Similarity Index**

**70%**

## Chapter 5-CYBER PHYSICAL SYSTEMS AND GAME THEOR...

### By: K. Kumari

Top of Form

Mode:                                                                                                                                                            

Bottom of Form

809 words / 11% - Internet from 17-Nov-2022 12:00AM

[assured-cloud-computing.illinois.edu](https://assured-cloud-computing.illinois.edu/files/2014/03/Game-Theory-with-Learning-for-Cyber-Security-Monitoring.pdf)

655 words / 9% - Crossref

[Rasim Alguliyev, Yadigar Imamverdiyev, Lyudmila Sukhostat. "Cyber-physical systems and their security issues", Computers in Industry, 2018](http://linkinghub.elsevier.com/retrieve/pii/S0166361517304244)

611 words / 8% - Internet from 22-Aug-2020 12:00AM

[mafiadoc.com](https://mafiadoc.com/review-on-cyber-physical-systems-ieee-xplore_597bc18b1723ddb28e072d6d.html)

537 words / 7% - Internet from 01-Jan-2022 12:00AM

["Game theory", Wikipedia, en, 2022](https://en.wikipedia.org/wiki?curid=11924)

537 words / 7% - Internet

[Chung, Key-whan. "Game theory with learning for cyber security monitoring", 2015](http://hdl.handle.net/2142/89157)

264 words / 4% - Crossref

[Amit Kumar Tyagi, N. Sreenath. "Cyber Physical Systems: Analyses, challenges and possible solutions", Internet of Things and Cyber-Physical Systems, 2021](https://doi.org/10.1016/j.iotcps.2021.12.002)

140 words / 2% - Internet from 21-Oct-2020 12:00AM

[link.springer.com](https://link.springer.com/chapter/10.1007%2F978-3-319-95246-8_27)

141 words / 2% - Internet from 16-Jul-2020 12:00AM

[www.slideshare.net](https://www.slideshare.net/hechares/managerial-decision-making-management-process)

125 words / 2% - Internet from 21-Jul-2022 12:00AM

[wikimili.com](https://wikimili.com/en/Repeated_game)

113 words / 2% - Internet from 21-Oct-2022 12:00AM

[digital.library.txstate.edu](https://digital.library.txstate.edu/bitstream/handle/10877/9284/SIDDIQUE-THESIS-2018.pdf?isAllowed=y&sequence=1)

64 words / 1% - Internet from 01-Dec-2017 12:00AM

[link.springer.com](https://link.springer.com/content/pdf/10.1007%2F978-3-319-25178-3.pdf)

106 words / 1% - Crossref

[Dario Bauso. "Game Theory: Models, Numerical Methods and Applications", Foundations and Trends® in Systems and Control, 2014](https://doi.org/10.1561/2600000003)

104 words / 1% - Internet from 02-Nov-2022 12:00AM

[coek.info](https://coek.info/pdf-a-comparative-study-of-applications-of-game-theory-in-cyber-security-and-cloud-c.html)

96 words / 1% - Internet from 15-May-2019 12:00AM

[quadrantmodelofreality.blogspot.com](http://quadrantmodelofreality.blogspot.com/2016/02/quadrant-model-of-reality-book-14_14.html)

93 words / 1% - Crossref

[Muammer Eren Sahin, Lo’ai Tawalbeh, Fadi Muheidat. "The Security Concerns On Cyber-Physical Systems And Potential Risks Analysis Using Machine Learning", Procedia Computer Science, 2022](https://doi.org/10.1016/j.procs.2022.03.068)

92 words / 1% - Internet from 23-Jul-2008 12:00AM

[self.zh.wikimiki.org](http://self.zh.wikimiki.org/en/prisoner's+dilemma)

84 words / 1% - Internet from 24-Oct-2021 12:00AM

[www.thinkswap.com](https://www.thinkswap.com/plag-scan/au/mq/psyu1101-introduction-psychology-i/social-psychology-notes)

64 words / 1% - Internet from 30-Sep-2019 12:00AM

[www.ideals.illinois.edu](https://www.ideals.illinois.edu/bitstream/handle/2142/89157/CHUNG-THESIS-2015.pdf?isAllowed=y&sequence=1)

57 words / 1% - Internet from 15-Nov-2019 12:00AM

[www.scribd.com](https://www.scribd.com/document/407955202/Artificial-Intelligence)

56 words / 1% - Internet from 15-Jun-2022 12:00AM

[www.studymode.com](https://www.studymode.com/v1/turnitin_essay/1351324)

50 words / 1% - Crossref

[Yang Liu, Yu Peng, Bailing Wang, Sirui Yao, Zihe Liu. "Review on cyber-physical systems", IEEE/CAA Journal of Automatica Sinica, 2017](https://doi.org/10.1109/JAS.2017.7510349)

44 words / 1% - Internet from 14-Aug-2021 12:00AM

[wikizero.com](https://wikizero.com/en/Stuxnet)

36 words / < 1% match - Internet from 12-Dec-2019 12:00AM

[asmedigitalcollection.asme.org](https://asmedigitalcollection.asme.org/risk/article/doi/10.1115/1.4045146/1065484/A-Game-theoretic-Approach-FOR-Defending-Cyber?searchresult=1)

35 words / < 1% match - Internet from 22-Jan-2023 12:00AM

[www.investopedia.com](https://www.investopedia.com/terms/n/nash-equilibrium.asp)

34 words / < 1% match - Internet from 15-Oct-2022 12:00AM

[www.coursehero.com](https://www.coursehero.com/file/111008095/chap-4docx/)

27 words / < 1% match - Internet from 03-Jun-2021 12:00AM

[www.wrpsa.com](https://www.wrpsa.com/game-theory-in-rock-paper-scissors/)

23 words / < 1% match - Internet from 04-Feb-2019 12:00AM

[educationvijay.com](http://educationvijay.com/admin-panel/study/subjectfile/1economics.docx)

23 words / < 1% match - Internet from 14-Jan-2023 12:00AM

[slideplayer.com](https://slideplayer.com/slide/17390090/)

22 words / < 1% match - Internet from 12-Oct-2022 12:00AM

[studentsrepo.um.edu.my](http://studentsrepo.um.edu.my/8283/6/siew_kian.pdf)

21 words / < 1% match - Crossref

[Hong-Seok Park, Risky Ayu Febriani. "Modelling a Platform for Smart Manufacturing System", Procedia Manufacturing, 2019](https://doi.org/10.1016/j.promfg.2020.01.118)

21 words / < 1% match - Crossref

[Lee T. Maccarone, Daniel G. Cole. "A Game-Theoretic Approach to Defending Nuclear Instrumentation and Control Systems From Cyber-Threats", Volume 4A: Dynamics, Vibration, and Control, 2018](https://doi.org/10.1115/IMECE2018-87713)

20 words / < 1% match - Internet from 18-Oct-2022 12:00AM

[www.routledgehandbooks.com](https://www.routledgehandbooks.com/doi/10.1201/9780429455759-3)

17 words / < 1% match - Internet from 30-May-2022 12:00AM

[candana.mymom.info](https://candana.mymom.info/what/what-is-a-nash-equilibrium-in-game-theory.php)

17 words / < 1% match - Internet from 26-Oct-2022 12:00AM

[dspace.cvut.cz](https://dspace.cvut.cz/bitstream/handle/10467/62066/F3-BP-2015-Jandova-Katerina-intelligent_algorithms_for_petrol_station_inspections.pdf)

10 words / < 1% match - Crossref

[Lee Maccarone, Daniel Cole. "A Game-theoretic Approach FOR Defending Cyber-physical Systems From Observability Attacks", ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg, 2019](https://doi.org/10.1115/1.4045146)

10 words / < 1% match - Internet from 26-Dec-2022 12:00AM

[docshare.tips](https://docshare.tips/game_58b30c1bb6d87f3b4d8b47e3.html)

8 words / < 1% match - Crossref

["Game Theory and Machine Learning for Cyber Security", Wiley, 2021](https://doi.org/10.1002/9781119723950)

8 words / < 1% match - Crossref

[Soumita Das, Anupam Biswas. "Deployment of Information Diffusion for Community Detection in Online Social Networks: A Comprehensive Review", IEEE Transactions on Computational Social Systems, 2021](https://doi.org/10.1109/TCSS.2021.3076930)

8 words / < 1% match - Internet from 09-Jun-2014 12:00AM

[www.docstoc.com](http://www.docstoc.com/docs/146868044/Econometrics)

7 words / < 1% match - Crossref

[Omid Torabi, Abbas Mirakhor. "3. Methodology", Walter de Gruyter GmbH, 2020](https://doi.org/10.1515/9783110582925-003)

7 words / < 1% match - Crossref

[Wang, B.. "Game theory for cognitive radio networks: An overview", Computer Networks, 20101006](https://doi.org/10.1016/j.comnet.2010.04.004)

6 words / < 1% match - Crossref

[Hamed Orojloo, Mohammad Abdollahi Azgomi. "A method for evaluating the consequence propagation of security attacks in cyber–physical systems", Future Generation Computer Systems, 2017](https://doi.org/10.1016/j.future.2016.07.016)

Cyber Physical Systems and Game Theory Integration Haritha Deepthi and Siddiq Moideen Department of Information Technology & Department of Computer Engineering, PSG PolytechnicCollege, Coimbatore, Tamil Nadu, India harithadeepthibtech@gmail.com; siddiqmoideen07@gmail.com

**Abstract: Cyber Physical Systems are**Multidisciplinary **Engineered Systems that rely on**

Computation, Communication & Control (3C) Technologies in-order to integrate Full-Fledged Physical System and Control & Computational Resources/Elements. Such that Cyberspace can Control & Alter Physical Environments. Thus, Exposing Physical Process

**to Cyber**-Threats. **An Attacker, who is able to access Control inputs can**affect **the system while remaining undetected**via **masking certain measurement signals**

& renders a portion of system unobservable, which is Observability Attack.Observability attacks can be analysed by Game-Theoretical approach. Where,

**Attacker’s Strategy Set includes all possible Masked Measurements**. Whereas, **Defender’s Strategy Set includes all possible Reinforcements**to defend **the**

system, which are further Quantified & Analysed. Eventually Multiple Nash Equilibria are identified; Thus, an Optimal Strategy can be used

**to defend Cyber Physical System from**an **Observability**Attack. Keywords: **Cyber Physical Systems**

, Hybrid Systems, Open System Interconnection, Real-time Systems, Industry 4.0, Cyber Twin,Heterogeneity,Parallelism, Nash Equilibrium, Prisoner’s Dilemma, Strategic form,Stochastic Game, Value of state, Quality of state, Minimax Q-Learning, Learning rate, Exploration rate, Naïve Q-Learning, Optimal policy INTRODUCTION TO CPS

**Cyber Physical Systems are multidisciplinary systems**that conductfeedback **control on widely distributed embedded**

computingsystems through

**combination of communication**, computationand **control technologies**. Modern **CPS**are **able to realize the real-time**, dynamic, **safe**and **reliable collaboration with physical systems represented**via **embedded system**

.They are Integral mixture

**of existing network systems and**traditional embeddedsystems. Where, **Physical**

systemdata

**modules collect data by distributed**fielddevices **in CPS system**

, then pass data to theinformation processing layer as per thecomplete given tasks and demands ofservicesby information processingtechnologies such asstatistical signal processing,feedback control, data security processing anddata uncertainty management. The potential benefits of the convergence of 3C technologies for developing next-generation engineered systems that can becalled Cyber Physical Systems are wide ranging and highly transformative viaefficient computation, distributed sensing, high-level decision-making algorithms, control over wireless / wired communication networksformal verification technologies andmulti- objective optimization; engineered cyber physical systems are in many societal critical domains such as construction, energy, transportation, andmedical systems.Scientists and Engineersin

**this field have deep understanding of system and**branches **of**mechatronics, **biology**, computer scienceand **chemistry**. Physical systems& **Technical**

systemsare developed and designed to bemore & more reliable, efficient,smart,robust and secure. Figure 1: CPS Framework CPSs coversa vast

**range of**applied **areas, which**allow designing **systems to be more economically by**shared design tools& **abstract knowledge**

. Which also

**allows designing more**& more **dependable cyber-physical systems to get by applying**the **best**methods **to the entire range of**cyberphysical **applications**thereby **the**economic **and**technologicaldrivers **are creating an**atmosphere **that**

enables wide range of application possibilities and opportunities.Advancements in CPSs has produced

**new generation of systems that rely on cyber-physical technology such as: • Automotive systems**• Avionics • **Assisted living • Critical infrastructure control**

• Distributed robotics • Defence systems • Environmental control •

**Energy conservation**• Process **control • Manufacturing • Medical**systems& **devices**• Traffic safety & **control • Smart structures**

With such high notions, the scope of CPS and integration of Cloud computing is about to bring the next big Industrial Revolution, Industry 4.0. The complete factory can be made into digital twin in the cyber space. Any changes in the cyber twin will reflect in the physical world which could boost the production & efficiency via varied implications. Figure 2: Digital Cloning via CPS implications Wireline and wireless data networks were non-existent decades ago. Therefore, advancements in CPS’s network technologiesisdestined to the third generation of control systems. There has also been enormousgrowth in the complexity of programming ,hardware andsoftwareabstractions andthere has alsobeen an enormous evolution of distributed systems in the field of control system. There is another aspect; Internet of Things, where physical objects areassigned uniqueaddresses and they are interconnected with each other,targeted on connecting the entities over the Internet. All of it combined leads to another platform revolution. In such high time, it is necessary to re-examine both the policies as well as standard mechanisms. By mechanisms, regulating & standardising theimplementation a system, while by policies, setting up a regulatory protocol. There are many challenges ahead that are to be addressed in the mere future; As technology evolves, the Cyber threats evolves too. Figure 3: Industry 4.0 Principles There can be a massive economic benefitwhichwill

**eventually bring fundamental**changes **to the**functioning **of**theexisting engineered **physical systems**

.The scientific research community defines Cyber-Physical Systemtechnology indifferent perspectives. Some describe

**the Cyber-Physical System as**engineeredphysical **systems designed with operations that are**monitored, **controlled and integrated by**thetelecommunication **and computing cores. The**CyberPhysical **System is deeply**intertwinedwith **the physical components that demands real-time response and**

are to be connected across technologies at different paradigms. Such descriptions at sight, the definition of CPS boils down to; “The Cyber-Physical Systemsare next generationengineered systems that are

**complex, integrated to become a part of the physical phenomena and is embedded with the existing computing technology”. As a system, the CPS is viewed as an engineering discipline that deals with**the **technology and the**modelling **of physical processes together with mathematical**&computational **abstractions. The CPS has been designed in a manner where there is an interaction between the**cyber **and the physical environment**. Figure 5: **CPS**

Block Diagram

**CPS interact with physical system through networks**, theend **system of CPS is normally traditional centralized**tightlycoupled **embedded computing system, which contains a**largenumber **of physical systems composed of intelligent**wired/ **wireless**actuators & **sensors**. CPS ARCHITECTURE **CPS**

**collects the information of physical world and transmits those information- to**

-cyber space,

**where information is processed and sent back to the physical world**. Thereby, **the hybrid system is a**basefor **CPS**

Hybrid systemin

**which continuous variables and discrete events**

in real-

**time and have mutual influence & interaction**

,

**but now there is no general model of hybrid system application. The**

CPS architecture encapsulates the two major components:

**the cyber layer & the physical layer**

.

**CPS includes variables that represent data obtained by sensors and control variables**that represent **control signals**

. Figure 6: Typical CPS Architecture In CPS, thestandard

**value of a certain process parameter is**referred to **set point**

,

**the distance between the values of the process variables and the corresponding control points**are **calculated by the controllers. After calculating**the **offset**value, **the controllers**, use **a complex set of equations**, to **develop a local actuation, and compute new actuation & control variables. the received control value is sent to the corresponding actuator to keep the process closer to a specific set point Controllers also send the received measurements to main control servers and execute the selected commands from them**

to perform the designated process. CPS’sHuman Machine Interface (HMI) which is Graphical User Interface (GUI) which is provides interactive platform with the system &

**current state of the controlled object to the human operator. General CPS process**

stages:

**1) monitoring; 2) networking; 3) computational processing; 4) actuation. The cyber layer often uses industrial protocols**

**to communicate with physical layer. A**

Cyber Physical System consists of multipleactuators and dynamic/static sensor networks integrated with the intelligent decision system.Different types of Cyber Physical Systems component

**integration are based on effective**communicationand **connectivity**

.

**CPSs are characterized by**heterogeneous information flow, **cross-domain sensor cooperation and intelligent decision making.CPS**

considers computational layer use information & knowledge from physical environmental input. CPS comprises vast combinations of key functions;

**depending on the field of application, the**further steps **arises & the**

requirement is fulfilled.The general

**architecture of CPS is divided into seven fundamental levels of**Open System Interconnection ( **OSI) model from the physical to application layer**

. Figure 7: OSI Layers Fundamental Architecture Levels

**Physical layer The physical layer lays groundwork for the CPS architecture. The physical layer consists of sensors& actuators**

whichreceives the analog signalsfrom the working physical environment, transforms into digital signals, then transmitted via wired\ wireless networks likeZigBee, Wi-Fi,2G/3G/4G, UWB, Bluetooth,RFID readers, 6LoWPAN, WiMAXand wired & tag technologies network protocolsthat are used in physical and data link layers.

**Devices at this level usually have**small **memory and processing power**

. These layers connect via Bluetooth, UWB &Internet. Thus,

**Attacks on this layer mainly come from external sources. Data link layer The data link**

**layer serves the network layer requests and uses the physical layer**services **to receive and send packets.The data link layer**

**provides the creation, transmission, and reception of data frames**. The data link **layer**

is divided into Logical Channel Management sublayer which

**provides network layer service and**Media Access Control **sublayer**which **regulates access to a shared physical environment. An attack on this layer can lead to disruption of MAC addresses, which could result in a failure of the device identification. Network layer**The network **layer**

**uses the IPv4/IPv6 and RPL protocols**to route **the**

packets via converting MAC addresses to network addresses.

**The attacks that lead to the failure of sensors and actuators, lead to a change of information and source from which it was obtained**which will **subsequently lead to a mechanical failure. Transport layer**The transport **layer**

uses TCP, UDP, and ICMP to break down the packets into small fragments.

**Attacks on this level lead to a decrease in the speed of network equipment**

which will subsequently lead to

**failure of services. Session layer The session layer**takes care of **communication session**

which is

**an integral part of the functions of the top three layers of the model**

.

**It monitors the order of message transmission over the network**

; inserts labels into long messages to handle exceptions, not to transmit from the beginning again. Presentation layer The presentation level uses

**Secure Socket Layer protocol, which provides secret message exchange for the application-layer protocols of the TCP/IP stack**

. Thus,

**coordinates the data presentation**i.e., syntaxin **the interaction of two application processes: data transformation from the**internal **format to**externalformat; **data encryption and decryption**

. Application layer The application layerstores,

**analyses and updates information received from previous**layersmakes **control decisions that can be visualized using the virtual prototype interface**

; thus,covering different domains.

**The protection of data privacy is the most important issue of this level**

. CPS CHARACTERISTICS& COMPLEXITIES Physical System

**Physical system is the important**half **of CPS**which **involves physical system design such as hardware design**,system testing, **hardware size and connectivity encapsulation**

andenergy management.

**Every physical system has its network characteristics as well as maximized multi-level network coverage, a variety of complex temporal and spatial scale to meet the time requirements of different tasks and a high degree of automation**

. Uncoordinated Change User and

**as well as the different parts of the CPS, need to be taken care of during the transition**

,which might expose the CPS to

**new vulnerabilities**that **could make the system less secure and could be a**bigger **problem for**

the organisationthis can be prevented by

**upgrading hardware, updating or changing applications, and adding new**far more secure **features**

.

**Pattern Abstraction Existing programming languages still lack**hardware abstraction, relevant **concurrency model**

andtemporal semantics.

**The changes of system theory requires the integration of the physical system theories including control systems, signal processing and the computing system theories**comprises of **complexity, scheduling**and **computation. the**

**temporality of network protocols becomes a key issue**

.

**Synchronized implementation of spatial and temporal theory in the computer systems. The collaborative interference and control of the state of physical process are achieved through embedded computer communication networks. The Bottom-up change of computer construction is the feasible approaches, which provides accurate**real time **capability**

which replaces

**the cache with the scratchpad memory buffer, developing**

concurrent and real-time software components,

**developing temporal semantic described programming languages**

,

**providing new technical means so that networks**that **can offer highly precise time synchronization**

and

**choosing appropriate concurrency models for the static analysis**

. The Top-down approach based on modelling i.e., using models to replacespecific

**programming language to express the**behaviour **of the system**

. Size &Computability

**Large scale CPS will involve many things in terms**such as number **of**units, connectors, lines- **of**-code, **logical interactions, requirements and stakeholders. Size related**aspects **can also be seen to encompass the**number **of**resources **needed to**

manufacture a product,

**the amount of information needed to describe an object and the**

computational complexity. Security by Design Since, components in CPS

**are not connected to other networks, like the internet**.Mostly **security isn't taken into account in the design of CPS**

. Physical security is theat mostprecautionfollowed to keep CPS safe in general.

**Due to the characteristic of network system and physical system being open, there**exists **problems**such as **invasion**, counterfeiting, **tampering, and other malicious attacks as well as delay in network transmission system, so CPS must be able to deal with the problem of security, effectiveness**, credibility, predictability, **dynamic**

andreal- time implementation.

**Identity of information collecting sources or control instruction senders must be authenticated, and the receiver must be able to exactly determine the real identity of the sender to prevent counterfeiting**

and preserve credibility.

**The accuracy of processing as well as the validity and integrity of information or instruction set must be guaranteed to prevent the uncertainties and noise in CPS processing from affecting the system processing accuracy**

to preserve Validity.Automatically adjusting

**rules and generate commands based on the task requirements and changes in external environments to eliminate bias and meet task requirements according to**pre-set **rules**

via dynamic reorganization and reconfiguration. Figure 8: Cyber Physical Attacks Both

**cyber and physical aspects**must be **taken into account**; that **could help us better predict and stop future cyber-attacks that have physical consequences, we need to build structures for both parts of the solution**i.e., **cyber-physical solution**

.

**A higher level of security reduces the risk of confidential information disclosure, provides data anonymity, and hides important information details. CPSs security protects the system from intrusions and reduces the likelihood of risks**

.

**There are several security design principles that can be useful in constructing control systems that can survive attacks**: diversity, **redundancy, principle of least- privilege and separation of privilege**

.

**Data confidentiality is provided by various security mechanisms**like **data encryption& two-factor authentication**. Such security mechanismsprotects **CPS sensor data from their disclosure and transferring to**any **unauthorized party**

. Figure 9: Holistic System Design Approach

**CPS sensors can measure physical properties and convert them into a signal.There are different types of sensors that perform different functions and are used in different areas**

. Real-time digital data are captured and areprocessed by the sensors.

**In some cases, they can also have a certain degree of memory, which allows them to register a certain number of measurements. Sensors with a low data transfer rate form, which are increasing in popularity, as they can have more sensor nodes than wired sensor networks and work offline for a long time**. Such as **machine-to-machine**(M2M) **communications, which are subject to additional security measures, based on their characteristics associated with different protocols and their applications**

to be secure & resilient.

**Security should be performed on all layers of the CPS architecture, from the physical layer to the application layer**

. Information System

**Information system is the core**in **CPS**

which comprises

**real-time system, network system, file system, hierarchical storage system, memory management, modular software design, concurrent design and formal verification**

. Engineered technicians in theinformation

**system can transform the information in physical system engineering into the rules and models of software system**

. Heterogeneity CPS represents distributed, hybrid, real-time and closed-loopsystems,

**thus requiring**engineers **to deal with a multitude of**behaviours, propertiesand **performance**

targetswhich must

**deal with the problem of time synchronization and space**allocation **of different components. CPS**

**are strongly characterized by heterogeneity in several dimensions**

, requirements, functions, technology andstakeholders. Due to such

**heterogeneity, CPS**are **typically be represented using multiple interdependent views, captured with different formalisms and tools**

.

**Traditional scheduling strategies cannot meet the requirements of real time CPS which have complex time semantic expression, although a variety of programming languages provide abundant time functions, but how to use these time functions to design scheduling strategy with practical awareness has become an open research problem**

.

**Widely applied which requires effective calculation and physical equipment performance optimization strategy. Aiming at predictable CPS realization and energy consumption**

,

**task scheduling of CPS based on feedback control**

,

**The demand model of computer science uses discrete mathematical description while the demand model of control theory is described by the differential equation and the**behaviour **of the system, therefore, discreteness and continuity needs to be combined when establishing models of CPS**

. Real-Timeliness Nature

**CPS involves the problem of time synchronization while the control theory at present cannot predict what will happen next. Most processing mechanisms of computer system are asynchronous, which just consider how to realize the function in**modelling **rather than when to implement. Therefore, CPS needs to find ways to integrate the two, otherwise the computing, communication and control capability in physical equipment cannot be realized**.The requirement **in**

**real time is a requirement that affects the state of defence if**real-time computation **isn't met. Networks that are under attack need to make quick decisions in CPS to**

preserve the stability of the system.

**That way, a CPS security design that takes into account the interactions between physical and cyber**

in real time. Even minor improvements in real time computation might lead to

**better risk assessment, threat detection**and **more**robust & **resilient solutions**

to defend the attack.

**There must be lightweight and hardware- based mechanisms built on top of cryptographic mechanisms to improve real-time interaction and deadlines**

. Dynamics

**CPS typically represent tightly**coupled **and**integrated **systems where the change of one parameter in the design is likely to influence many other parameters and also**

**requires consideration of dynamics and structure at multiple levels or scales**

.

**Due to highly non-linear and coupled dynamics**, orstructural **aspects such as dependencies among parts and properties**

.

**Parallelism in**the **terms of concurrent cyber and physical parts, and resource sharing in the computer systems**furthercontribute **to complexity**

. REAL-WORLD CYBER PHYSICAL THREATS

**Cyber (C), Cyber-Physical (CP), and Physical (P)attacks on a number of CPS applications that harm CPS systems**

. They very hard toget

**back or figure out what happened right away. Attacks are grouped**respectively **based on where the injuries are. Attacks that**target & **hit**

the system’s software & internal level and not the sensors & actuators are categorised into “Cyber Attacks”. Attacks that physically target & hit the system’s components in real world are categorised into “Physical Attacks”. Attacks that target & hit the system’s physical layer which affects and alters the existing real-world by means of cyberspace& masking techniques are categorised into “Cyber Physical Attacks”. Real-World Occurrences Smart Monitoring System Attack User’s safety would at risk if a wearable device, home-assist devices or any smart device’s security is breached. The attacker can actively monitor record the moves of the victim via the breached systemfor their own gain. Industrial Control System Attacks CPSs are applied in wide arrange of field, such as aviation, water treatment systems, nuclear plants, construction, sewage system, industries, etc. any considerable vulnerability in the system could lead to catastrophic failure. Stuxnet-2010,

**attack on Iran's nuclear power plants**

that

**caused damage to several nuclear plants**

which could have also been a Threat to whole world in result, it was due to a Security breakthrough.

**Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Stuxnet's design and architecture are not domain-specific and it could be tailored as a platform for attacking modern SCADA and PLC systems**

. This breakthrough

**ruined almost one-fifth of Iran's nuclear centrifuges**. This **worm infected over 200,000 computers and caused 1,000 machines to physically degrade**

. Smart Grid CPS Attack Attackers can do cyberattacks on Smart grids and Blackout an entire state or a country. This make destabilize the complete system & economy and social life of the affected areas would crumble. Smart Monitoring System Attack User’s safety would at risk if a wearable device, home-assist devices or any smart device’s security is breached. The attacker can actively monitor record the moves of the victim via the breached systemfor their own gain.

**Medical CPS attack A distributed system is**very **vulnerable**toinsider attacks& **cyber-spies**

.An intruder can

**harm people by jamming the wireless signals that medical devices use to keep**

victim in health and the attacker can damage or tamper the medical deviceand make machines do what the attacker wants to. Smart Vehicles Attacks Car manufacturers

**are trying to come up with new technologies that will make their cars more useable**, comfortable **and**safe **for their customers**

. CPS is an important facet in current industry standard cars. As technology evolves, chances of security breaches gets bigger too. If an attacker could break into the system, Vitim’s life could be in danger.

**GAME THEORY Game Theory is**primarily **a**mathematical frameworkanalyses the **decision- making**

of a player based on how they expect other players to make a decision i.e., determining optimal rational choices given a set of circumstances which

**can be applied in many fields such as economics**

, politics, computer science, biology, philosophy & so on.

**Game theory depicts the game played between different players and the strategies of each player. A game can be defined as interaction of different players according to a set of rules. Players may consist of individuals, machines**, parties, **companies or associations. The results of game theory depends**upon behaviour **of**every other **player**

present in the game and not only the current player.

**Due to this reason, this approach is extremely scalable and versatile. The outcome of game theory also depends on the estimated payoff by each player before making decisions, which is a measure of the satisfaction obtained by each player by making that decision**. Therefore, **the players will perform actions and take decisions**that **would provide them**the **maximum payoff**

.

**Game A (strategic form) game is a tuple (N**,(Ai) **i∈N**,(ui) **i∈N), where • N = {1, 2, . . ., n} is the set of players**(maximisers), • **Ai is the set of actions of player i, • A := {a| a**= (ai) **i∈N**, ai∈ Ai, ∀ **i∈ N} is the set of action**profiles, • **ui: A → R is the payoff function of player i, i.e., (a1, . . . , an) → ui(a1, . . . , an). Payoff ui is a profit (to maximize) but can also be a cost(to minimize). An equivalent way of writing the action profiles is (aj )j∈N= (a1, . . . , an) = (ai, a−i), where a−i**= (aj) **j**∈N, **j≠i is the action profile of all players**

excepti. Normal and Extensive form Representation

**The normal \ strategic form game is usually represented by a matrix which shows the players, strategies, and**payoffs. **More generally it can be represented by any function that associates a payoff for each player with every possible combination of actions**. If **there are two players; one chooses the row and the other chooses the column. Each player has two strategies, which are specified by the number of rows and the number of columns. The payoffs are provided in the interior. The first number is the payoff received by the row player**

;

**the second is the payoff for the column player**

.

**When a game is presented in normal form, it is presumed that each player acts simultaneously or, at least, without knowing the actions of the other**

. Figure 10: Normal Form

**If players have some information about the choices of other players, the game is usually presented in extensive form.Every extensive-form game has an equivalent normal-form game, however, the transformation to normal form may result in an exponential blow-up in the size of the representation, making it computationally impractical**

.

**The extensive form**can be **used to formalize games with a time sequencing of moves**represented like tree. **The extensive form can**

**also capture simultaneous- move games and games with imperfect information**

. Here each vertex/ noderepresents

**a point of choice for a player. The player is specified by a number listed by the vertex. The lines out of the vertex represent a possible action for that player. The payoffs are specified at the bottom of the tree. The extensive form can be viewed as a multi-player generalization of a decision tree. To solve any extensive form game, backward induction must be used. It involves working backward up the game tree to determine what a rational player would do at the last vertex of the tree, what the player with the previous move would do given that the player with the last move is rational, and so on until the first vertex of the tree is reached**

. Figure 11: Extensive Form

**Types of games In game theory**, there are **different types of games**that **help**

us analyse different problems. They are categorised in

**the basis of number of players involved**, cooperation among players & **symmetry of the game**

. Figure 12:

**Game Types Cooperative &Non-cooperative**Games **A game is cooperative if the players are able to form binding commitments externally enforced**maybe **through contract law. A game is non-cooperative if players cannot form alliances or if all agreements need to be self-enforcing**maybe **through credible threats. Cooperative games are often analysed through the framework of cooperative game theory**

and

**provides a high-level approach as it describes only the structure& strategies**

**which focuses on predicting which coalitions will form, the joint actions that groups take, and the resulting collective payoffs**

. he

**traditional non-cooperative game theory**is more general **which focuses on predicting individual**player’s **actions and payoffs and**analysing **Nash equilibria. The focus on individual payoff can result in a phenomenon known as Tragedy of the Commons, where resources are used to a collectively inefficient level**

.

**Non- cooperative game theory also looks at how bargaining procedures will affect the distribution of payoffs within each coalition**

.

**While using a single theory may be desirable, in many instances insufficient information is available to accurately model the formal procedures available during the strategic bargaining process, or the resulting model would be too complex to offer a practical tool in real world. In such cases, cooperative game theory provides a simplified approach that allows analysis of the game at large without having to make any assumption about bargaining powers**

.

**Nash Equilibrium Nash equilibrium is a concept in game theory**

in which every participant

**in a non- cooperative game**can optimize their **outcome**based on **the**

other player’s decisions which is achieved in a game when

**no player has any incentive**for deviating **from their**own **strategy**

, even if they know the other player’s strategies. It

**is a decision-making theorem within game theory that states a player can achieve the desired outcome by not deviating from their initial strategy**but based on **the**

actions of other players. Therefore, used to predict the best response in any given situation.

**In the Nash equilibrium, each player's strategy is optimal when considering the decisions of other players. Every player wins because everyone gets the outcome they desire**

.

**Prisoner’s Dilemma The prisoner's dilemma is a standard example**; how **game analysed in game theory**which **shows why two completely rational individuals might not cooperate, even if it appears that it is in their best interests to do so**

.

**Prisoner's dilemma**is a **situation where individual decision-makers always have an incentive to choose in a way that creates a less than optimal outcome for the individuals as a group. Two members of a**

cartel named Robert & Walterwere

**arrested and imprisoned. Each prisoner is in solitary confinement**and they have **no means of communicating with**each **other. The prosecutors lack sufficient evidence to convict the pair on the principal charge**

. Figure 13: Decision Matrix Prosecutors hope to get both of them sentenced

**on a lesser charge. Simultaneously,the prosecutors offer each prisoner a bargain. Each prisoner is given the opportunity either to betray the other by testifying that the other committed the crime or to cooperate with the other by remaining silent. The**options offered **are: • If**Robert&Walter, both **betray**each **other**

**i.e., if they both confess, each of**themserves 10 **years in prison. • If**Robert **betrays**Walter **but**Walter **remains silent**, Robert **will be set free**&Walter must **serve**

50years

**in prison. • If**Walter **betrays**Robert **but**Walter **remains silent**, Walter **will be set free**& Robert must **serve**50 **years in prison. • If**Robert&Walter **both remain silent, both of them will only serve 1 year in prison**

. Note that

**it is implied that the prisoners will have no opportunity to reward or**punishtheir **partner other than the prison sentences they get and that their**decisionwill **not affect their reputation in the future**

. We’d feel both remaining silent would be the best option. But they will not opt it. Both of them will betray each other i.e., they would confess. Because that is the human psychology, this feels the best option for both the parties. Individually the prisoner clings on luck that he would be

**set free, if the other**prisoner **does not confess**

& fears that what if I remain silent and the other confesses.

**Because betraying a partner**offersa **greater reward than cooperating with them, all purely rational self**-interestedprisoners **will betray the other, meaning the only possible outcome for two**purelyrational **prisoners is for them to betray each other**

and that is Nash Equilibrium.

**The prisoner’s dilemma game can be used as a model for many real-world situations involving cooperative behaviour. The label "prisoner’s dilemma" may**beapplied **to situations not strictly matching the formal criteria of the classic**oriterative **games; for instance, those in which two entities could gain**importantbenefits **from cooperating or suffer from the failure to do so, but find it**difficultor **expensive**but **not necessarily impossible to coordinate their activities**

. Zerosum &

**non-Zero sum Games Zero-sum games**

/

**constant-sum games**are games **in which choices by players can neither increase nor decrease the available resources. In zero-sum games, the total benefit**goes **to all players in**a **game, for every combination of strategies, always adds to zero. Poker exemplifies a zero-sum game, because one wins exactly the amount one's opponents lose.Zero-sum games**

usuallycorrespond

**to activities like**gambling **and**theft, **but not to the fundamental economic situation in which there are potential gains from trade. It is possible to transform any constant-sum game into**anasymmetric **zero-sum game by adding a dummy player called**as " **the board" whose losses compensate the**player’s **net winnings**

.

**Other zero-sum games include**heads or tails **and most classical board games**such as **chess.Many games studied by game theorists including the prisoner's dilemma are non-zero-sum games, because the outcome has net results greater or less than zero. In non-zero-sum games, a gain by one player does not necessarily correspond with a loss by another**. Simultaneous & Sequential **Games**

**Simultaneous games are games where both players move simultaneously, or instead the later players are unaware of the earlier**player’s **actions**

,

**normal form is used to represent simultaneous games**

.

**Sequential games / dynamic games are games where later players have some knowledge about earlier actions. This need not be perfect information about every action of earlier players; it might be very little knowledge. For instance, a player may know that an earlier player did not perform one particular action, while they do not know which of the other available actions the first player actually performed**

,

**extensive form is used to represent sequential games**

**Multiple extensive form games correspond to the same normal form. Consequently, notions of equilibrium for simultaneous games are insufficient for reasoning about sequential**

**games. Symmetric & Asymmetric**Games **A symmetric game is a game where the payoffs for playing a particular strategy depend only on the other strategies employed, not on who is playing them**. That is, **if the identities of the players can be changed without changing the payoff to the strategies, then a game is symmetric. Many of the commonly studied**2×2 **games are symmetric. The standard representations of the prisoner's dilemma, and the stag hunt are**the **symmetric games. Asymmetric games are games where there are not identical strategy sets for both players. For instance, the**dictator **game**

andultimatum

**gamehave different strategies for each player. It is possible, however, for a game to have identical strategies for both players, yet be asymmetric**

. DEFENSE-ATTACK MODEL In modelling a defence in CPS,

**we are considering parties**witha **conflict of interests: the attacker and the defender**. Thedefender, often **the system administrator, manages the system.The main interest of the defender is to secure the cyber**& physical **infrastructure from malicious activities. The attacker**, is **the**

**malicious opponent who attempts to compromise**thetarget **system**. So, **we model the interaction between the**attackerand **the defender based on data on actual security incidents**

.

**Defender The defender is a party that is in charge of making proper responses to secure the**CPS **from malicious attacks. The defender has a set of monitors to protect the system. The main objective of this player is to make proper responses in a**pre- emptive **manner based on a limited view of the system status, relying on monitors**

in the CPS design. Defence

**State DSx represents the state of the attack from the defender’s**perspective. **The observations that defenders use rely on the monitoring systems, and lack the granularity**i.e., **the**level **of**

data in database

**needed to reveal the details of**user’s **actions. Defender Action D is a set of actions available to the defender in a given state. For security incident detection and response, a monitor detects changes in system status. However, such detections do not directly map to the attacker’s definite actions. The monitor may miss an action or misidentify a benign action**on CPS **as**a **malicious**attackwhich would be **false**negative or false **positive. Hence, the defender needs to take an appropriate action while relying on imperfect information. Assuming that there are proper responses for each action, we**must regulate & **abstract the defender action to**either Respond **or**

Not Respond.

**Attacker The attacker is an opponent who accesses the system**withthe **intention of threatening its security. Attacks can vary**froma **single action to a sequence of activities**

. welimit

**our interest to attacks that consist of multiple**activitiesthat **lead to an ultimate goal**

of breaking into the CPS.

**Attack State ASx represents the state of the attack, i.e.,the depth/degree of intrusion. Each attack state is**assigneda **numeric value**i.e., **reward which**quantifies **the damage to**thetarget CPS. **The**bigger **the**impact, **the more severe**

thedamage

**to the system and/or the greater the**unauthorizedcontrol **over the system. Transition from one state to**anotherdepends **on the result of the action. Activity ‘A’ is a set of actions**aiavailable **to the attacker.It can lead to malicious control over the**CPS, **or if**theattacker **decides to remain in the current state, the**transitionwill **result in a loop. The set of available activities in state**ASxis **denoted by Ax. Therefore, Ax is a subset of A. The**causalrelation **between activities and attack states represented**via **a state diagram. Transition Matrix Pa(s, s’) is the probability that an**actionfrom **state s will lead to a transition to the next state s’. In**anattack **model, a transition matrix represents the probability**ofa **successful attack on**

CPS. Depending on themonitoring

**system configured on the defender’s side, an attack can be either**detectedor **missed. The transaction matrix models the uncertainty**ofthe result **of an action.Immediate**RewardRa(s, s') **is the reward of the**attackeras **a result of a**transition **from state s to s’ for**performingaction **a. The reward is a quantitative representation of**theearnings that **the attacker can get from a successful attack**. Attacker- **Defender**

**interaction While each attacker has a logic flow for making decisions**, the players **decisions are not independent, but**they **are related to the opponent’s decision process. Hence, we model the interaction between the two players**

.

**Once an attacker has taken an action, the defender chooses**their **action based on the information from the monitoring system. An attacker’s action results in a transition to the intended state only if the defender does not make a proper response. Once the defender has responded to the observed action, the attacker is forced to transit to the default state. Assuming a zero-sum game, a successful attack will result in an immediate reward, and the defender will have a symmetric loss. As a result of the execution of the attack, the attack state will change accordingly. Otherwise, if the defender detects the attack and makes a proper response, the attack state will be reset to the default for the identified attacker**

. Therefore,

**reward will be assigned to the defender, with an equivalent loss**for **the attacker. GAME MODEL**

IMPLIMENTATION

**The game consists of two**or more **rational players with conflict**, andtheir **goal is to maximize their reward by deriving the**optimalpolicy **for each state**. concepts **of**

**quality of state and value of state are introduced to represent the expected reward of the player’s decision**

in each game model. Stochastic Game Stochastic game / Markov gameis

**a repeated game with probabilistic transitions played by one or more players. The game is played in a sequence of stages. At the beginning of each stage the game is in some state. The players select actions and each player receives a payoff that depends on the current state and the chosen actions. The game then moves to a new random state whose distribution depends on the previous state and the actions chosen by the players. The procedure is repeated at the new state and play continues for a finite or infinite number of stages. The total payoff to a player is often taken to be the discounted sum of the stage payoffs or the limit inferior of the averages of the stage payoffs**. Set of actions **A**

**contains all possible actions, a that**areavailable **to the player. We use o for the opponent’s action.Reward R(s, a, o) defines the immediate reward based on**theattack **state s and player’s actions, a and the opponent’s**actiono **in the**

t-thiteration.The concepts ofquality

**of state and value of state are introduced to**representthe **expected reward of the player’s decision. Value of state V(s) is the expected reward when the player,starting from state, follows the optimal policy. It is**equivalentto **the maximum reward that the player can expect**, assumingthat **the opponent’s action o will be the action that**minimizesthe expected reward. **The**player maximizes **the value of**stateby **deriving the optimal policy, i.e., the probability**distributionamong **the actions available to the player in a given state. 𝑉**(𝑟) = **max**min ∑ **𝜋**

(𝑟, 𝑎′)𝑄(𝑟, 𝑎′, 𝑜′) 𝜋 𝑜′∈𝑂𝑠 𝑎′∈𝐴𝑠

**Discount factor γ is assigned by the user’s intention on balancing between future and current rewards. A player, who only considers current reward, is**modelled **by a value of 0 while 1 is assigned for a player who strives for a long-term high reward**

.

**Quality of state Q(s, a, o) is the expected reward each**playercan **gain by taking actions a and o from state s and**thenfollowing **the optimal policy from then on. The quality of**stateis **a sum of the immediate reward from this iteration (Rt−1)and the reward expected as a result of transitioning to**

states’ (Vt(s’),

**which was derived from the previous t iterations.Note that the value of state is weighted by a discount factor(γ**). 𝑄𝑠+ **1**(𝑟, **𝑎,**) = 𝑄𝑠+1( **𝑟, 𝑎, 𝑜**

) + 𝛾𝑉𝑠(𝑟′)

**Optimal policy π is the set representing the probability distribution of actions (π(s, .)) available at each state(s). It**ischosen **to maximize the value of state(V(s)) which**representsthe **expected reward of the player if the player follows**theoptimal **policy. π(s, a) indicates the likelihood of taking**actiona **in**states **where π is the overall distribution that**maximizesthe **value of state (V(s)). 𝜋**(𝑟, . ) = **𝑎𝑟𝑔 max**min ∑ **𝜋**

(𝑟, 𝑎′)𝑄(𝑟, 𝑎′, 𝑜′) 𝜋′(𝑠,.) 𝑜′∈𝑂𝑠 𝑎′∈𝐴𝑠 Minimax Q-Learning

**In a security game, the assumption of complete**informationand **rationality is even more unrealistic**. Generally, **players make decisions with limited information**, andcompensate **for their lack of information with learning**

. Therefore,

**Minimax Q-Learning as a decision-making algorithm**. Insteadfor **a need of complete information on the attack model**, theMinmax **Q-Learning algorithm allocates partial weight on**itsearlier **results to combine knowledge of history, the**actualearnings **on the current iteration, and the future**expectedreward. **Quality of state Minimax Q-Learning**

embeds

**the learning aspect into the algorithm**. 𝑄𝑠+ **1**(𝑟, **𝑎,**) = 𝛼𝑄𝑠(𝑟, **𝑎, 𝑜) + (1**− 𝛼)𝑄𝑠+1( **𝑟, 𝑎, 𝑜**

) + 𝛾𝑉𝑠(𝑟′)

**Learning rate α leverages the ability of the player by**assigninga **real value between 0 and 1. A learning rate of**

0 representsfull

**learning ability for the player while a rate of**1modelsthe case where **the player only considers only the most**recentinformation. **In full learning, the player would not**considerthe **immediate reward R(s, a, o) and the expected future**awardV( **ns) but keep the quality of state constant. To account**forthe **absence of prior results to learn from at the initial**stageof **the game, an α of 1.0 is assigned; α then decays as Q(s,a, o) accumulates information on the performance of**previousiterations. **Exploration rate exp is a distinct parameter for which determines the degree of variation from the**optimalpolicy. **Unlike the Markov game, in which the optimal**solutionis **known from the initial iteration, Q-Learning has to**learnthe **optimal policy by trial and error. The exploration**ratedetermines the relative **rate**of **the**

**action not following**theoptimal **policy to learn the results of different actions. An**expvalue **closer to 0 results to a**Markov **game while a value**closerto **1 means that the player will take random actions. Naive Q-Learning In a security game, information about the opponent is**notalways **available. The attacker often has information about**thetarget **system from public resources. However, the amount**ofinformation **is limited. Similarly, the defender is playing**agame **against an unspecified opponent. In order to model**thissituation, **Naive Q- Learning from is applied. Naive Q-Learning optimizes the strategy without information about**theopponent, such as **the opponent**

’

**s action o. It utilizes**limitedinformation **of the immediate reward and its own**informationto **derive the optimal policy. Quality of state updated accordingly to reflect the**

limitedinformation.

**the opponent’s action is no**longerconsidered **for differentiating the Quality of state**. 𝑄𝑠+ **1**(𝑟, ) = 𝛼𝑄𝑠(𝑟, **𝑎) + (1**− 𝛼)𝑄𝑠+1( **𝑟, 𝑎**

) + 𝛾𝑉𝑠(𝑟′)

**Value of state The maximum expected reward when following the optimal policy**

. Due to lack ofinformation

**about the opponent, o is no longer considered. 𝑉**(𝑟) = **max ∑ 𝜋**(𝑟, **𝑎**′)(𝑟, **𝑎′) 𝜋 𝑎**

′∈𝐴𝑠′ Optimal policy

**optimal policy that maximizes the**valueof **state (V(s)). the quality of state (Q) is**onlydefined **for s and a but not o. 𝜋**(𝑟, . ) = **𝑎𝑟𝑔 max**min ∑ **𝜋**(𝑟, **𝑎′)𝑄**(𝑟, **𝑎′) 𝜋′(𝑠**,.) 𝑜′∈𝑂𝑠 **𝑎**

′∈𝐴𝑠 Using these Game Models, whether we know or do not know the information / strategy of the opponent who’s about to attack CPS, as per the requirement & previous trials the respective game model can be chosen.Securing maximum value of state from the defender’s perspective, CPS can be defended from the cyber physical attack. CONCLUSION

**Cyber Physical Systems are**Multidisciplinary **engineered systems that**could transform **the**

lens we see upon world. As the system advances, the x times the growth of security threats. Game Theory is decision making mathematical framework that can be implied in various sectors. One of the major implications are in Cyber Security. Based on the number of players, strategy & situation the respective game theoretical model can be chosen to defend the threats from the attacker. Thus, securing the CPS.