Abstraction

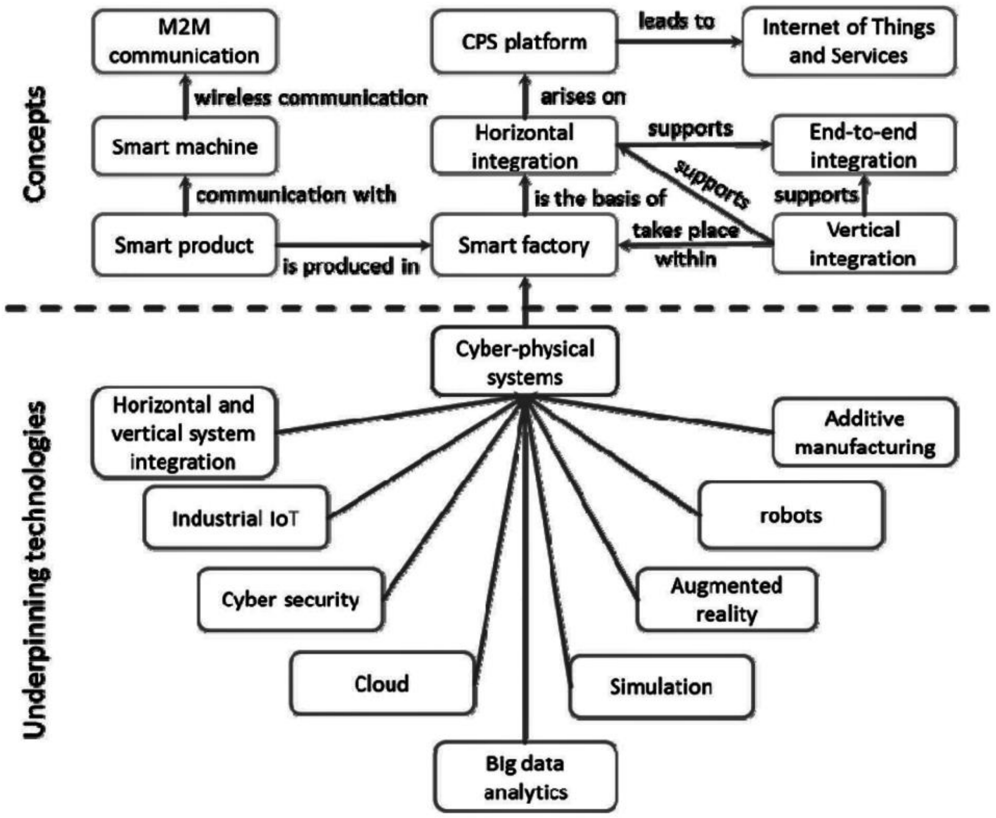
Cyber Physical Systems are Engineered Systems that rely on Computation, Communication & Control (3C) Technologies in -order to integrate Full-Fledged Physical System and Control & Computational Resources/Elements. Such that Cyberspace can Control & Alter Physical Environments. Thus, Exposing Physical 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 & render a portion of state space unobservable. This is known as 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 Measurement Reinforcements, 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.

INTRODUCTION TO CPS

Cyber Physical Systems are multidisciplinary systems that conduct feedback control on widely distributed embedded computing systems through combination of computation, communication and control technologies. Modern CPS are able to realize the Realtime, safe, reliable and dynamic collaboration with physical systems represented by embedded system. They are Integral mixture of existing network systems and traditional embedded systems. Where, Physical system data modules collect data by distributed field devices in CPS system, then pass data to the information processing layer according to the demands of services and complete given tasks by information processing technologies such as feedback control, statistical signal processing, data security processing and data uncertainty management.

The potential benefits of the convergence of 3C technologies for developing next-generation engineered systems that can be called Cyber Physical Systems are Highly transformative and wide ranging. Through real-time embedded systems for distributed sensing, efficient computation, and control over wired / wireless communication networks, high-level decision-making algorithms, multi-objective optimization, and formal verification technologies; engineered systems in many societal critical domains such as construction, energy, transportation, and medical systems. Scientists and Engineers in this field have deep understanding of system and branches of mechatronics, computer science, biology and chemistry & working of the field environment. Physical systems & Technical systems can be designed and developed to be more & more reliable, secure, smart, robust and efficient.

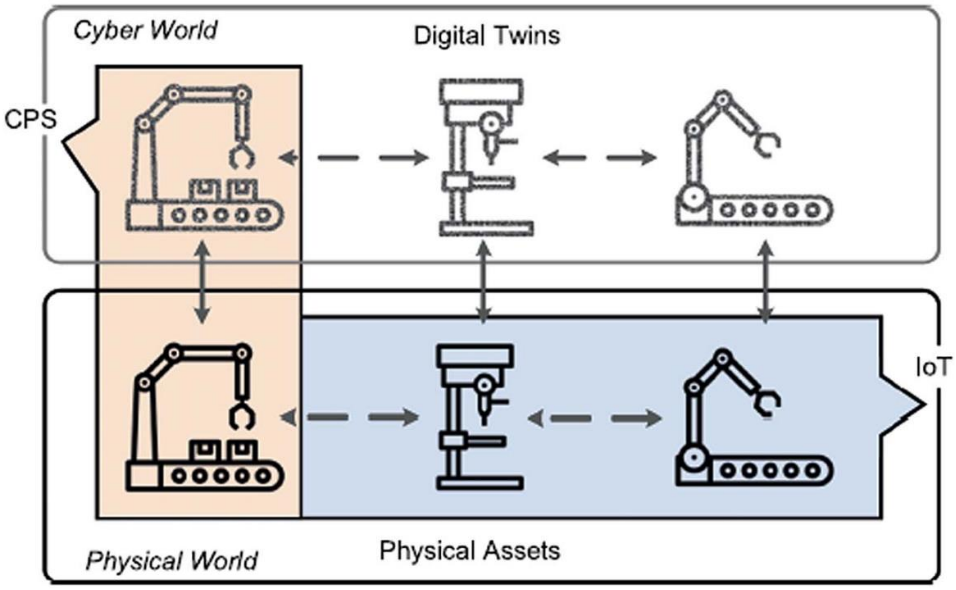


CPSs cover an extremely wide range of application areas, which allow designing systems to be more economically by shared design tools and abstract knowledge. This allows designing more & more dependable cyber-physical systems to get by applying the best methods to the entire range of cyber-physical applications whereby the technological and economic drivers are creating an environment 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:

- Advanced automotive systems
- Assisted living
- Avionics
- Critical infrastructure control

- Defence systems
- Distributed robotics (telepresence, telemedicine)
- Energy conservation
- Environmental control
- Manufacturing
- Medical devices and systems
- Process control
- Smart structures
- Traffic control and safety

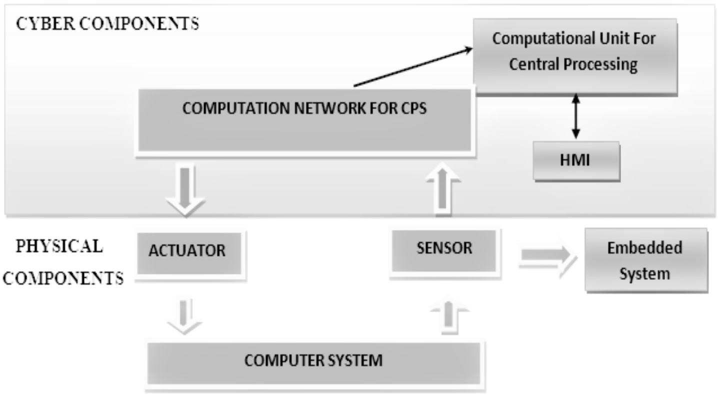
With such high notions, the scope of CPS and integration of Cloud computing is about to bring the next big Industrial Revolution, Industry 4.0. The complete factory can be made into digital twin in the cyber space. Any changes in the cyber twin will reflect in the physical world which could boost the production & efficiency via varied implications.



Wireline and wireless data networks were non-existent decades ago. Thus, the emergence of networked CPSs is leading to the third generation of control systems. There has also been enormous growth in the complexity of hardware, software and in the programming abstractions that have been developed for building them. There has been evolution in the technology of control system implementations on distributed systems. In process control, the controller area network has been used to provide the underlying communication network for distributed control systems. There is another aspect; Internet of Things, where physical objects are assigned addresses and interconnected with each other, with interest therefore focused on the communication physical system interface. All

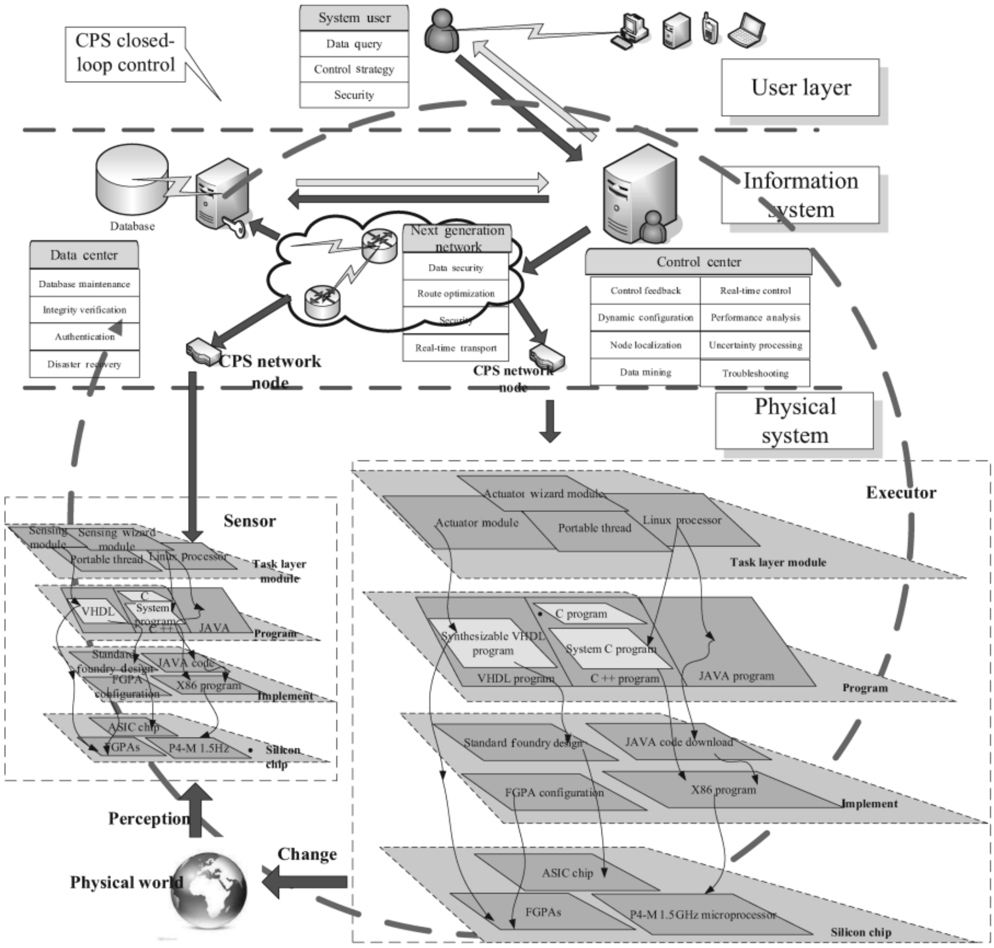
this, together, constitutes yet another platform revolution. At such a time of platform revolution, it is necessary to examine both mechanisms as well as policies. By mechanisms, regulating & standardising the implementation a system, while by policies, setting up a regulatory protocol. There are many challenges ahead that is to be addressed in the mere future; As technology evolves, the Cyber threats evolves too.
CPS can also bring huge economic benefits and will eventually bring fundamental change to the functioning of the existing engineered physical systems. The scientific community researching the Cyber-Physical System has defined technology with *different perspectives*. Some of them have described the Cyber-Physical System as engineered and physical systems designed with operations that are controlled, monitored, and integrated by the computing cores and telecommunication. The Cyber-Physical System is deeply intertwined with the physical components that it demands a real-time response and that in most cases, the system is distributed across a given array of connected technologies. As such, the descriptions regarding the Cyber-Physical System boil down to one definition; the Cyber-Physical System is a next generation engineered system that is 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 technology and the modelling of physical processes together with computational & mathematical abstractions. The CPS has been designed in a manner where there is an interaction between the cyber and the physical environment.

CPS interact with physical system through networks, the end system of CPS is normally traditional centralized tightly coupled embedded computing system, which contains a large number of physical systems composed of intelligent wired/wireless actuators & sensors.



CPS ARCHITECTURE

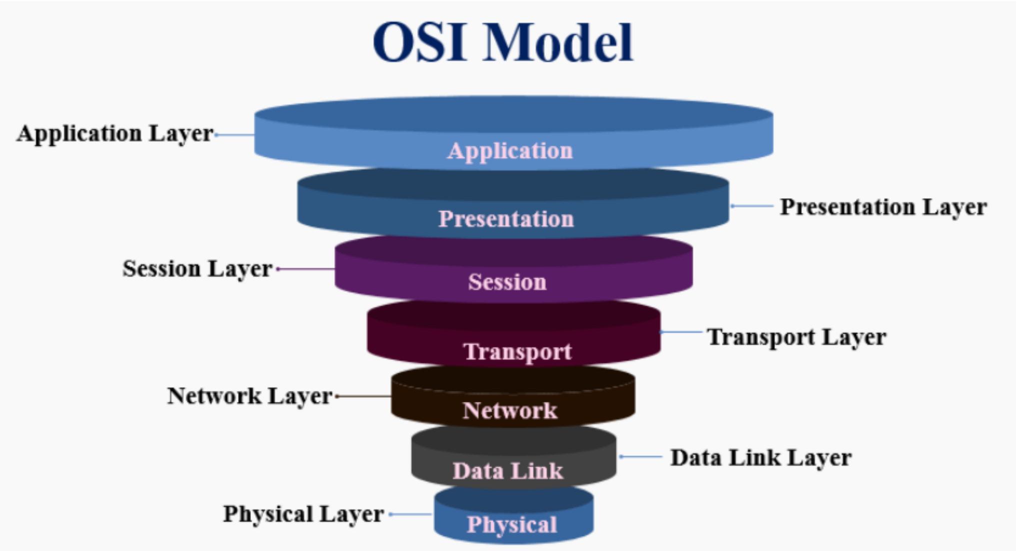
CPS collects the information of physical world (continuous variable) and transmits those information-to-information world (discrete event), where information is processed and sent back to the physical world. Therefore, the hybrid system is a foundation of CPS Hybrid system refers to those systems in which continuous variables and discrete events exist at the same time and have mutual influence and interaction, but now there is no general model of hybrid system application.



The CPS architecture encapsulates the two major components: the cyber layer and the physical layer. CPS includes variables that represent data obtained by sensors and control variables representing control signals. In CPS, the normal value of a certain process parameter is called a set point, the distance between the values of the process variables and the corresponding control points is calculated by the controllers. After calculating this the offset value, the controllers, using a complex set of equations, 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's graphical user interface (GUI), called the human-machine interface (HMI), 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 CPS may consist of multiple dynamic/static sensor and actuator networks integrated with intelligent decision system. Different types of CPS components integration are based on effective connectivity and communication. CPSs are characterized by cross-domain sensor cooperation, intelligent decision making and heterogeneous information flow. CPS considers computational components that use common knowledge and information from physical environmental input. CPS includes various combinations of key functions and depends on their applications. Depending on the field of application, the issue arises which of the characteristics should be used and to what extent. The CPS architecture can be considered at various levels. The most common architecture of CPS is divided into seven fundamental levels of Open System Interconnection (OSI) model from the physical layer to the application layer.



Fundamental Architecture Levels

Physical layer

The physical layer lays groundwork for the CPS architecture. The physical layer consists of sensors & actuators which receives the analog signals from the working physical environment, transforms into digital signals, then transmitted via wireless or wired networks. For example, 2G/3G/4G, Wi-Fi, UWB, ZigBee, Bluetooth, RFID readers, 6LoWPAN, WiMAX and tags & wired technologies (PLC, NC, etc.) is a network layer protocol and can be used with any physical and data link layer. Devices at this level usually have small memory and processing power. This layer is used to connect ZigBee, Bluetooth and other systems to the 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., syntax in the interaction of two application processes: data transformation from the internal format to external format; data encryption and decryption.

Application layer

The application layer stores, analyses and updates information received from previous layers makes 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 and energy 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 organisation this 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 and temporal 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 replace specific programming language to express the behaviour of the system.

Size & Computability

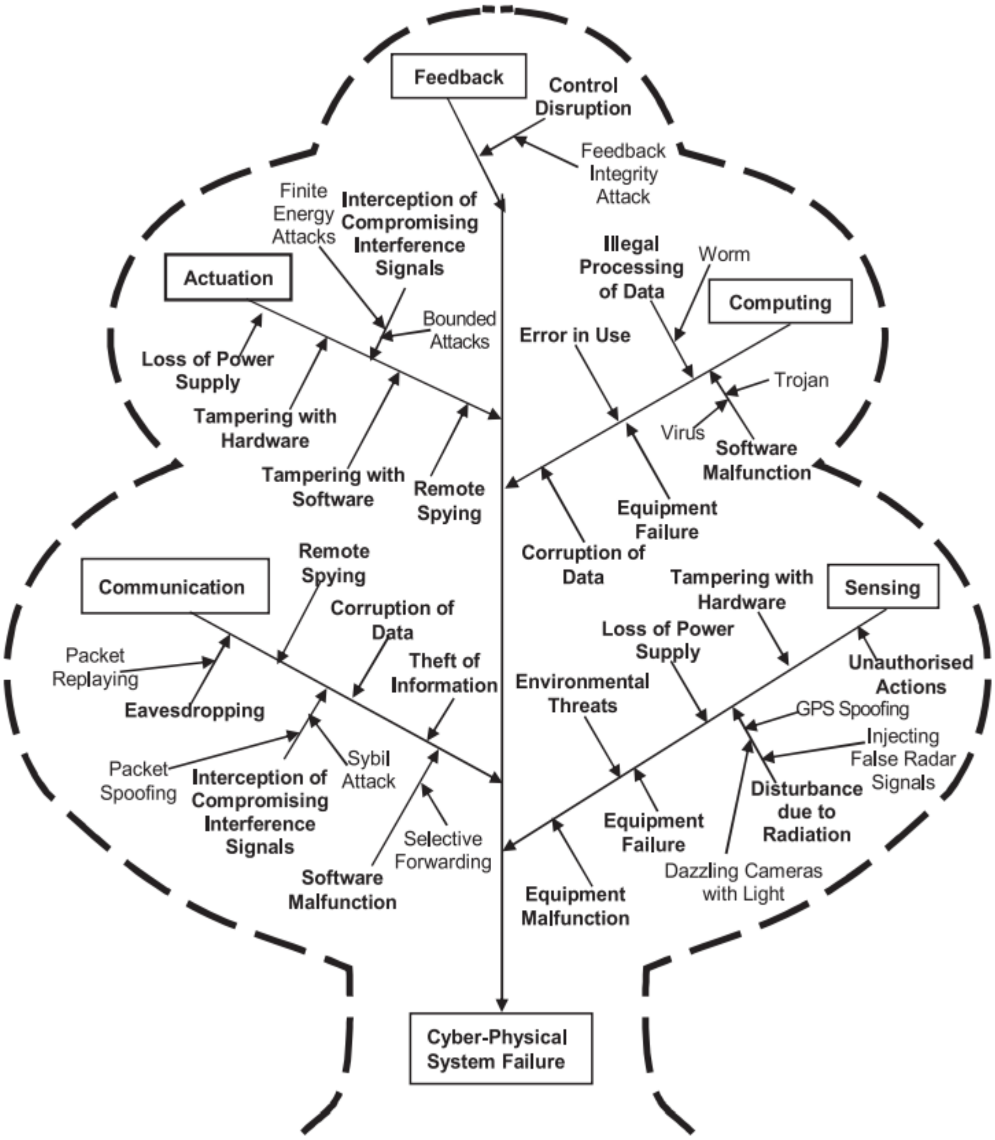
Large scale CPS will involve many things in terms such as number of units, connectors, lines-of-code, logical interactions, requirements and stakeholders. Size related aspects can also be seen to encompass the number of resources needed to manufacture a product, the amount of information needed to describe 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 the at most precaution followed 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 and real-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.

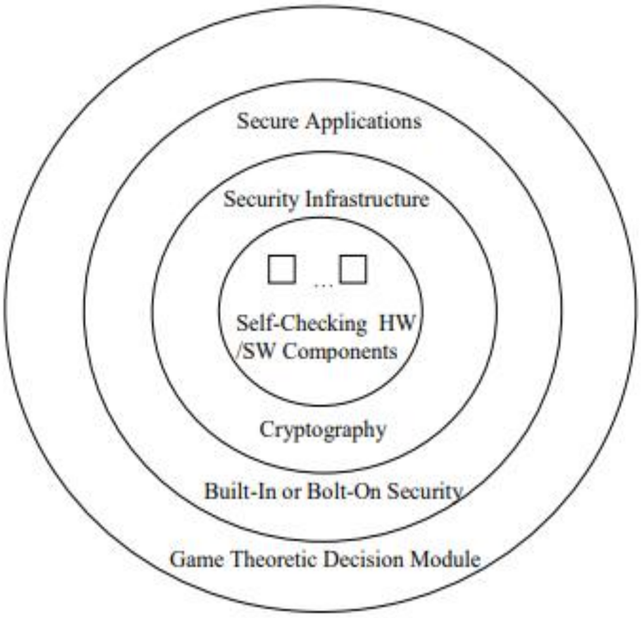
Both cyber and physical aspects must be taken into account; that could help us better predict and stop future cyber-attacks that have physical consequences, we need to build structures for both parts of the solution i.e., cyber-physical solution. A higher level of security reduces the risk of confidential 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 mechanisms protects CPS sensor data from their disclosure and transferring to any unauthorized party.

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 are processed 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.


Secure Applications
Security Infrastructure
□ ... □
Self-Checking HW /SW Components
Cryptography
Built-In or Bolt-On Security
Game Theoretic Decision Module

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 the information 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-loop systems, thus requiring engineers to deal with a multitude of behaviours, properties and performance targets which 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 and stakeholders. 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, or structural 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 further contribute 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 to get 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 system for 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 system for their own gain.

Medical CPS attack

A distributed system is very vulnerable to insider 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 device and 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 framework analyses 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 $(N, (A_i)_{i \in N}, (u_i)_{i \in N})$, where

- $N = \{1, 2, . . ., n\}$ is the set of players (maximisers),
- A_i is the set of actions of player *i*,
- $A := \{a| \ a = (a_i)_{i \in N}, \ a_i \in A_i, \ \forall_i \in N\}$ is the set of action profiles,
- $u_i : A \to \boldsymbol{R}$ is the payoff function of player *i*, i.e.,

$$(a1, . . . , an) \to u_i(a_1, . . . , a_n).$$

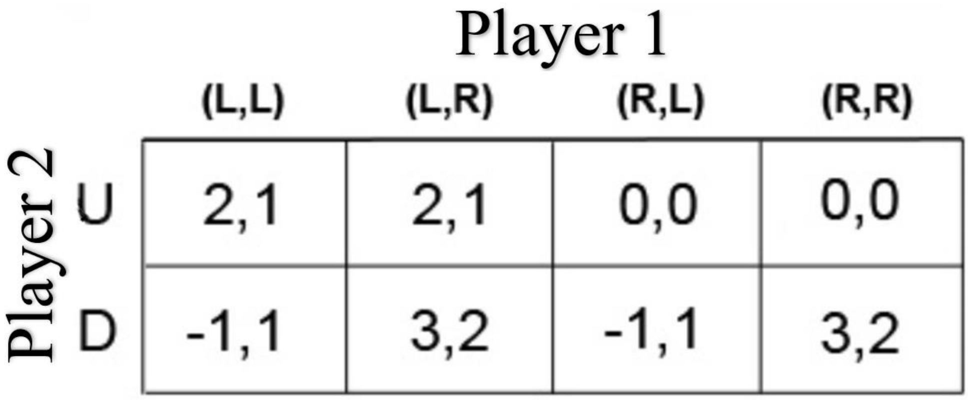
Payoff u_i is a profit (to maximize) but can also be a cost(to minimize).
An equivalent way of writing the action profiles is

$$(a_j \ )_{j \in N} = (a_1, . . . , a_n) = (a_i, a_{-i}),$$

where $a_{-i} = (a_j \ )_{j \in N}, j \neq i$ is the action profile of all players except *i*.

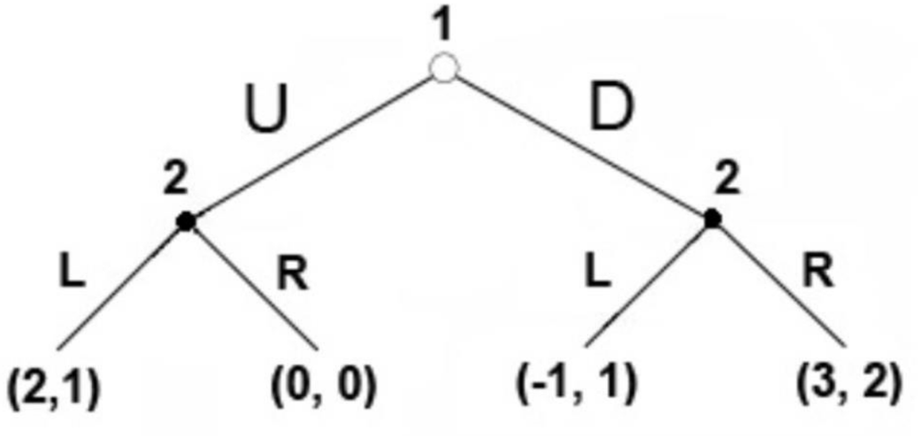
Normal and Extensive form Representation

The normal (or 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.



		Player 1			
		(L,L)	(L,R)	(R,L)	(R,R)
Player 2	U	2,1	2,1	0,0	0,0
	D	-1,1	3,2	-1,1	3,2

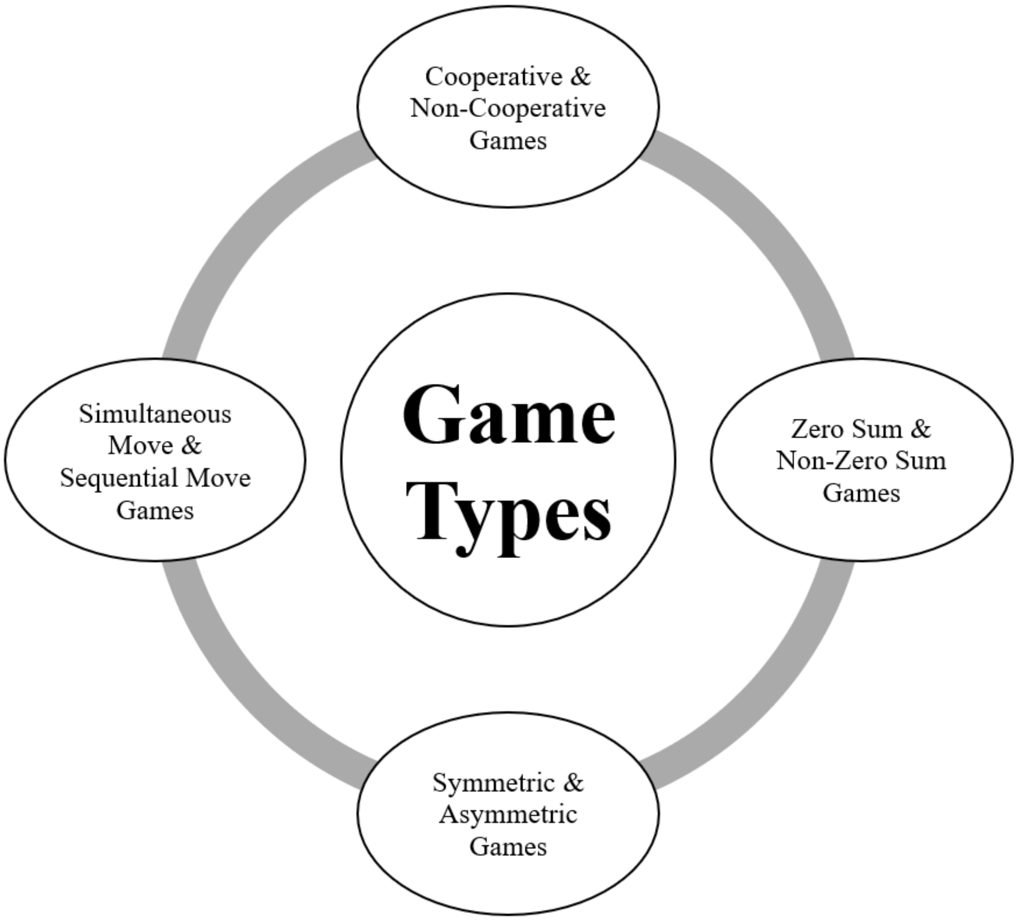
If players have some information about the choices of other players, the game is usually presented in extensive form. Every extensive-form game has an equivalent normal-form game, however, the transformation to normal form may result in an exponential blow-up in the size of the representation, making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

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.


Cooperative & Non-Cooperative Games
Simultaneous Move & Sequential Move Games
Game Types
Zero Sum & Non-Zero Sum Games
Symmetric & Asymmetric Games

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

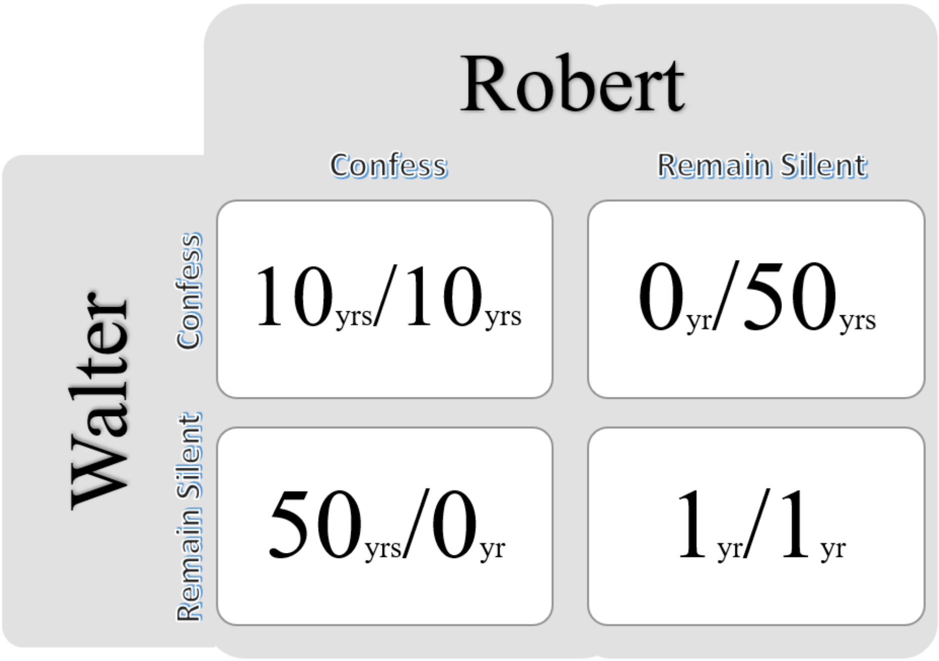
Nash equilibrium is a concept in game theory in which every participant in a non-cooperative game can optimize their outcome based on the other player’s decisions which is achieved in a game when no player has any incentive for deviating from their own strategy, even if they know the other player’s strategies. 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.



		Robert	
		Confess	Remain Silent
Walter	Confess	$10_{yrs}/10_{yrs}$	$0_{yr}/50_{yrs}$
	Remain Silent	$50_{yrs}/0_{yr}$	$1_{yr}/1_{yr}$

Two members of a cartel named Robert & Walter were 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.

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 them serves 10 years in prison.

- If Robert betrays Walter but Walter remains silent, Robert will be set free & Walter must serve 50 years 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 punish their partner other than the prison sentences they get and that their decision will not affect their reputation in the future.

We’d feel both remaining silents 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 offers a greater reward than cooperating with them, all purely rational self-interested prisoners will betray the other, meaning the only possible outcome for two purely rational prisoners is for them to betray each other.

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 be applied to situations not strictly matching the formal criteria of the classic or iterative games; for instance, those in which two entities could gain important benefits from cooperating or suffer from the failure to do so, but find it difficult or expensive but not necessarily impossible to coordinate their activities.

Zero sum & 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 usually correspond 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 a asymmetric 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 and ultimatum game have 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, we are considering parties with a conflict of interests: the attacker and the defender.

The defender, 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 the target system. So, we model the interaction between the attacker and 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 system 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.

Defence State

DS_x 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 needed to reveal the details of users' 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 as malicious which 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 with the intention of threatening its security. Attacks can vary from a single action to a sequence of activities. In this paper, we limit our interest to attacks that consist of multiple activities that lead to an ultimate goal.

Attack State

AS_x represents the state of the attack, i.e., the depth/degree of intrusion. Each attack state is assigned a numeric value(reward) which quantifies the damage to the target system. The bigger the impact, the more severe the damage to the system and/or the greater the unauthorized control over the system. Transition from one state to another depends on the result of the action.

Activity

'A' is a set of actions a_i available to the attacker. It can lead to malicious control over the system, or if the attacker decides to remain in the current state, the transition will result in a loop. The set of available activities in state AS_x is denoted by A_x. Therefore, A_x is a subset of *A*. The causal relation between activities and attack states represented via a state diagram.

Transition Matrix

$P_a(s, s')$ is the probability that an action from state *s* will lead to a transition to the next state *s'*. In an attack model, a transition matrix represents the probability of a successful attack. Depending on the monitoring system configured on the defender's side, an attack can be either detected or missed. The transaction matrix models the uncertainty of the result of an action. Immediate Reward $R_a(s, s')$ is the reward of the attacker as a result of a transition from state *s* to *s'* for performing action *a*. The reward is a quantitative representation of the earnings 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

The game consists of two rational players with conflict, and their goal is to maximize their reward by deriving the optimal policy 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 model

Stochastic Game

Stochastic game / Markov game is 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 are available to the player. We use o for the opponent's action. Reward *R*(*s*, *a*, *o*) defines the immediate reward based on the attack state *s* and player's actions, a and the opponent's action *o* in the *t*-th iteration. The concepts of quality of state and value of state are introduced to represent the 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 equivalent to the maximum reward that the player can expect, assuming that the opponent's action *o* will be the action that minimizes the expected reward. The player maximizes the value of state by deriving the optimal policy, i.e., the probability distribution among the actions available to the player in a given state.

$$V(s) = \max_{\pi} \min_{o' \in O_s} \sum_{a' \in A_s} \pi(s, a') Q(s, a', o')$$

Quality of state

Q(*s*, *a*, *o*) is the expected reward each player can gain by taking actions *a* and o from state *s* and then following the optimal policy from then on. The quality of state is a sum of the immediate reward from this iteration (R_{t-1}) and the reward expected as a result of transitioning to state s' (Vt (s0), which was derived from the previous t iterations. Note that the value of state is weighted by a discount factor (γ).

$$Q^{t+1}(s, a, o) = R^{t+1}(s, a, o) + \gamma V^t(s')$$

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.

Optimal policy

π is the set representing the probability distribution of actions ($\pi(s, .)$) available at each state(s). It is chosen to maximize the value of state($V(s)$) which represents the expected reward of the player if the player follows the optimal policy. $\pi(s, a)$ indicates the likelihood of taking action a in states where π is the overall distribution that maximizes the value of state ($V(s)$).

$$\pi(s, .) = \arg \max_{\pi'(s,.)} \min_{o \in O_s} \sum_{a' \in A_s} \pi(s, a') Q(s, a', o')$$

Minimax Q-Learning

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

Therefore, Minimax Q-Learning as a decision-making algorithm. Instead for a need of complete information on the attack model, the Minmax Q-Learning algorithm allocates partial weight on its earlier results to combine knowledge of history, the actual earnings on the current iteration, and the future expected reward.

Quality of state

Minimax Q-Learning embeds the learning aspect into the algorithm.

$$Q^{t+1}(s, a, o) = \alpha Q^t(s, a, o) + (1 - \alpha) R^{t+1}(s, a, o) + \gamma V^t(s')$$

Learning rate

α leverages the ability of the player by assigning a real value between 0 and 1. A learning rate of 0 represents full learning ability for the player while a rate of 1 models the case where the player only considers only the most recent information.

In full learning, the player would not consider the immediate reward *R*(*s*, *a*, *o*) and the expected future award *V*(*ns*) but keep the quality of state constant. To account for the absence of prior results to learn from at the initial stage of the game, an *α* of 1.0 is assigned; *α* then decays as *Q*(*s*, *a*, *o*) accumulates information on the performance of previous iterations.

Exploration rate

exp is a distinct parameter for which determines the degree of variation from the optimal policy. Unlike the Markov game, in which the optimal solution is known from the initial iteration, Q-Learning has to learn the optimal policy by trial and error. The exploration rate determines the relative rate of the action not following the optimal policy to learn the results of different actions.

An exp value closer to 0 results to a Markov game while a value closer to 1 means that the player will take random actions.

Naive Q-Learning

In a security game, information about the opponent is not always available. The attacker often has information about the target system from public resources. However, the amount of information is limited. Similarly, the defender is playing a game against an unspecified opponent. In order to model this situation, Naive Q-Learning from is applied. Naive Q-Learning optimizes the strategy without information about the opponent, such as the opponent's action *o*. It utilizes limited information of the immediate reward and its own information to derive the optimal policy.

Quality of state

updated accordingly to reflect the limited information. the opponent's action is no longer considered for differentiating the Quality of state.

$$Q^{t+1}(s,a) = \alpha Q^{t}(s,a) + (1-\alpha)R^{t+1}(s,a) + \gamma V^{t}(s')$$

Value of state

The maximum expected reward when following the optimal policy. Due to lack of information about the opponent, *o* is no longer considered.

$$V(s) = \max_{\pi} \sum_{a' \in A_s} \pi(s,a')Q(s,a')$$

Optimal policy

optimal policy that maximizes the value of state (*V*(*s*)). the quality of state (*Q*) is only defined for *s* and a but not *o*.

$$\pi(s,.) = \arg\max_{\pi'(s,.)} \sum_{a' \in A_s} \pi(s,a')Q(s,a')$$

Using these Game Models, whether we know or do not know the information / strategy of the opponent, as per the requirement & previous trials the respective game model can be chosen. Securing maximum value of state from the defenders perspective, CPS can be defended from the cyber physical attack.