**5G Cellular Network in Cyber Physical System: An Overview**

Trivikrama Bhat

trivikrama.16cs099@sode-edu.in

Vinaya

vinaya.15cs112@sode-edu.in

Shrikara

shrikara.16cs088@sode-edu.in

Rama Moorthy H

ramamoorthy.cs@sode-edu.in

***Department of Computer Science and Engineering,***

***Shri Madhwa Vadiraja Institute of Technology Management, Bantakal****.*

***Abstract: Cyber-physical systems are becoming more and more commonplace nowadays. It's expected that the cyber-physical systems revolution will be more transformative than the IT revolution of the past four decades. The world is expecting over 50 million sensors to be connected to the internet by 2020. This explosive increase in the number of connected ‘things’ needs to be accommodated in the available network architecture and infrastructure. Such a move is bound to be ridden with challenges that the cellular providers need to handle in order for all the millions of devices to work seamlessly. In this paper, we present an analysis of the current architecture of the connected CPS devices and mainly focus on how the next-generation 5G cellular networks enable CPS communications. (Security write)***

***Keywords: 5G, Cyber-Physical System, IoT.***

1. **Introduction**

Introducing the 5G cellular network for Cyber-Physical Systems and security considerations. Cyber-Physical Systems are integrations of computation with physical processes. The computing elements coordinate and communicate with sensors that monitor cyber and physical indicators, and actuators which modify the cyber-physical environment. The physical nature of the cyber-physical systems tends to expose information flow at the cyber-physical boundary. Along with a computational and physical component, all CPS systems by nature always contain a human component from design and development all the way through to the deployment and maintenance[1]. All these three components can be a potential vulnerability. In this paper, we examine the various challenges that are to be overcome in order to provide a secure environment for the operation of CPS devices.

Implementing CPS in cellular networks involves some challenges[2]. Although using cellular networks provides ubiquitousness, global connectivity, and security a few challenges are to be addressed. In current cellular networks, the mobile devices follow the control from base stations for spectrum access and communication and are not designed to handle large amounts of traffic. Moreover, the number of radio resources are already scarce and limited to traditional human communications. However, many of these challenges can be addressed by the specifications and technologies of future 5G networks.

The 5G Cellular Network is introduced to society for the enhancement in the fast and responsive communication of mobile and wireless communication systems. On these criteria, the network slicing is introduced in the cellular network which promises the future framework that enhances the technological and business requirements of industries. The CPS is architecturally supported by the 5G that offers the system to interact with the physical world and also process the data and communicate the information between the distributed elements like cloud and IoT in an end-to-end design. Most of the devices in a CPS system are in close proximity to each other. The problems faced in cellular networks can be overcome by implementing Device-to-Device(D2D) communication between the close proximity devices so that they can communicate directly with each other without the involvement of an intermediate Base Station.

To support massive machine-type devices (MTDs) is one of the main driving forces of 5G networks. In most of the current Machine Type Communication systems, MTDs communicate directly with the base station. This single-hop paradigm may not be able to support massive MTD where hundreds or thousands of MTDs attempt to set up communications. Furthermore, MTDs located at the boundary of a cell suffer from a high outage probability due to the interference from other MTDs. A costly solution is to deploy more base stations and split a cell into multiple small cells. Instead of investing a huge amount of money on deploying extra base stations or relays, cooperative communication has been demonstrated as an efficient and effective way to extend the coverage region and improve the throughput of cellular networks.

Developing and deploying a CPS system efficiently is not sufficient in the modern scenario. All components of a CPS system are either directly or indirectly associated with the physical world. Hence, defenses against both cyber and physical attacks should be present[3]. If not, having cybersecurity will only allow fake and malicious devices to connect to a system. As pointed out in [3] there are certain cyber-physical attacks that are geared towards causing some physical consequence. A clear example of this kind of attack is in the December 2015 attack on the Ukranian power grid[4]. The hackers targeted the power plant’s IT systems to gain access that infected the computers on the plant’s business network. They eventually gained access to the Industrial Control Systems(ICS) and caused circuit breakers to open up at a number of substations. The end result of this left around 2,25,000 customers without power for several hours in the middle of winter. Also, in [4] the authors have pointed out the various vulnerabilities introduced when distributed computing is employed for the management of a power system. Flexible AC Transmission System (FACTS) devices collectively, manipulate entire CFPS in a decentralized way, making distributed decisions to control the power system. This is proved in [4] to have a number of security vulnerabilities. It is clear from these examples that critical infrastructure components of a system that are part of a Cyber-Physical Network when compromised lead to serious physical consequences. In this paper, we also examine the security considerations to be made when implementing CPS in the cellular network.

# General Architecture of CPS

Traditionally the 5C (Connection, conversion, Cyber, Cognition, and Configuration) architecture[4] is employed for the cyber-physical system design.



Fig1 : The 5C of CPS

*2.1 Smart connection:* free method to manage data acquisition procedure and transferring data to the central server is required.

*2.2 Data to information conversion*:

Meaningful information has to be inferred from the data. Currently, there are several tools and methodologies available for the data to information conversion level. In recent years, the extensive focus has been applied to develop these algorithms specifically for health management applications. By calculating health value, estimated remaining useful life and etc. The second level of CPS architecture brings self-awareness to machines (Fig. 2).

* 1. *Cyber:*

The cyber level acts as a central information hub in this architecture. Information is being pushed to it from every connected machine to form the machine's network. Having massive information gathered, specific analytics have to be used to extract additional information that provides better insight into the status of individual machines among the fleet. These analytics provide machines with self-comparison ability, where the performance of a single machine can be compared with and rated among the fleet.

* 1. *Cognition:*

Implementing CPS upon this level generates a thorough knowledge of the monitored system. Proper presentation of the acquired knowledge to expert users supports the correct decision to be taken. For this level, proper info- graphics are generally used to completely transfer acquired knowledge to the users.

* 1. *Configuration*:

The configuration level is the feedback from physical space and acts as supervisory control to make machines self-configure and self-adaptive. This stage acts as a resilience control system (RCS) to apply the corrective and preventive decisions, which has been made in the cognition level, to the monitored system.

1. **Shifting CPS To 5G Cellular Networks**

The 5G system will be able to provide services and applications to the largest number of mobile devices in the history of cellular communication. The following are some of the services that 5G is expected to offer in the Acquiring accurate and reliable data from machines and their components is the first step in developing a Cyber- Physical System application. The data might be directly measured by sensors or obtained from the controller. Considering various types of data, a seamless and tether-coming days[6]:

1. Enhanced Mobile Broadband(eMBB)
2. Massive Machine-Type Communications(mMTC)

CPS devices are expected to highly rely on the range of services that are provided by the 5G cellular network. They are going to use these to communicate with the various distributed elements of the system such as the cloud, or an IoT infrastructure in an end to end manner.

Data processing is an important aspect of CPS, but not as important as analysis and useful information extraction. The large volume of data is first broken into workflows, so they can be easily distributed across multiple data centers, where different virtual machines can be run on them. This enables the parallel execution of tasks and queries for better data management, as well as the sharing of computing and storage resources through rental by users in a pay-as-you-go fashion.

Realizing CPS communications over D2D links can help achieve multiple benefits for future 5G networks[8]. First, to relieve spectrum congestion from signaling overhead caused by a massive number of physical objects attempting to communicate over licensed cellular bands, D2D technology solution allows the objects to share the cellular spectrum similar to cognitive radio networks (CRNs), but with some differences. First, while spectrum holes in CRNs are in the temporal domain, those in the cellular spectrum are in the spatial domain. This means that there is a spatial region around a D2D user where no cellular transmitter should be present to protect the cellular’s transmissions. By exploiting these spatial spectrum holes, both spectrum efficiency and power efficiency can be significantly increased. Second, CUs and D2D users are considered wireless users operating in two different modes: cellular mode and potential D2D mode; and therefore do not act as primary users and secondary users like in CRNs. Finally, D2D users can rely on the BSs for assistance in spectrum sharing.



# Fig 2: The D2D architecture

1. **Security Challenges In CPS Systems**

The interconnections between the CPS and IT systems have created exploitable security vulnerabilities[5]. Some of the factors that affect the emergence of these vulnerabilities are weak information security applications on CPS, the tendency of CPS to prioritize operational availability at the expense of integrity and confidentiality. It is to be noted here that attacks against CPS can cause physical damage to the real world. An apparent example where interconnected Information Technology(IT), and CPS network vulnerabilities led to severe consequences was the December 2015 cyber-attack on the Ukranian power grid as mentioned in the introduction.

Originally, CPS did not place a high priority on the information assurance techniques and processes that were originally developed to protect information technology systems. For IT systems in most businesses, the prioritization of these components of the information assurance is usually Confidentiality, Integrity, and Availability (the CIA triad). The reason for this order is the reliance of most businesses on confidentiality to protect trade secrets, contractual information that provide a competitive advantage in the marketplace. In [metro reference] the authors have described the problems due to legacy systems used within the CPS framework’s critical infrastructures and processes. The impact of disruptions and disturbances of legacy systems is far greater causing disruption to business operations, potential damage, and destruction to the equipment, operations, having serious adverse effects on society and human life. Despite these systems’ crucial social impact, the security protections of the majority of them are not on par with emerging attacks, since legacy systems may contain out-of-date devices that cannot support full- fledged security mechanisms. In fact, most of them have been deployed for a long time without getting and structural update. Many of the legacy systems were designed and implemented without conducting thorough studies on possible cyber and physical attacks, or even having no feasible counter-measures against such attacks. In addition, legacy systems usually include devices or parts that are exposed in physically unprotected spots, thus increasing the risk of cyber- physical attacks and insider attacks due to compromised devices.

Securing smart cyber-physical systems such as those based on IoT is comparatively hard[cite ergonomics paper]. Such smart systems aim to intelligently automate a variety of functions, with the goal of hiding that complexity from the user. Furthermore, the interactions of the user with such systems are more often implicit than explicit, for instance, a pedestrian with wearables walking through a smart city environment will most likely interact with the smart environment implicitly through a variety of inferred preferences based on previously provided automatically collected data.

The authors in [11] have given a very comprehensive study of the various security trade-offs that come into picture because of the newer security features and mechanisms introduced in most modern cyber physical systems. An instance of one such event was mentioned in a case where cars from a European manufacturer were reportedly being stolen extensively all over the world. This, on later investigation was found out to be the side effect of one of the security features implemented in the cars’ doors which made them unlock if a certain large amount of force was applied on the car’s roof assuming that the car has rolled over. So, basically, all the thief had to do was to jump on the car. Another safety critical CPS device the authors have studied greatly are Implantable Medical Devices (IMD). These devices are embedded into a patient’s body to simulate the function of a malfunctioned organ or to monitor the functions of some vital body parts. IMDs may also transfer data about the patient’s health and receive information to administer specific therapies. On one hand, the nature of the exchange information makes IMDs critically vulnerable to a wide range of threats that may affect the patient's life and thus the necessity for controlling their access using authentication protocols is absolute. On the other hand, in case of emergency where the patient might be incapacitated, these devices must allow communication with unauthenticated programmers to allow doctors to administer the required treatment which can save the patient's life.

# Implementation Using Case Studies

Consider 2 case studies, each explaining three different cases of CPS being used[8]. The case studies are explained using two scenarios.

* + 1. *The Remote Monitoring of the Vehicle*

In modern days people often wish to use cars now and then. Modern cars these days contain adequate computing capacity to perform complex processing. Processors of high capacity which are used in the gaming platform are also used within a car to perform AI functionality. The future enhancement will be carried out by introducing onboard units(OBUs) which will from specific purpose units designed for services such as speed control to generic networked nodes, like a network router, providing the ability to connect more devices. Therefore the OBU guarantees the connectivity with the infrastructure using the wireless interfaces and also expected that OBUs in the future will be provided by the industries as modern connectivity means. In our case, it assumes that the On-Board Unit (OBU) of the vehicle has some threshold capacity to host and execute container technology such as Docker. Such an OBU is what is also called nowadays in 5G a Mobile Edge Computing device (MEC). Internally this MEC will contain a south interface for communication and retrieving vehicle data through the Onboard device interface, while on the other side, it will offer a 5G new radio interface. The study of container technology will help us to deploy services in a secure way and easy configuration with the OBU is established.

The North Interface of the Automotive MEC provides connectivity form the car to External Service Providers(ESP).



# Fig. 4.1

For the above scenario, which displays, it is required to create and establish a communication path between the vehicle and the operator's cloud, to retrieve monitoring data from the vehicle and store them to services located at the operator’s premises. Since this provisioning scenario is expected to be common cases in future they need to be orchestrated and provisioned by modern 5G service software stacks, like a MANO, to offer flexibility and easy integration with the rest of the operator’s 5G infrastructure.

Ideally, the operator from the BSS/OSS (operations support system/business support system) side should create a so-called Network Service Descriptor (NSD), containing Virtual Network Functions(VNFs) that the MANO will automatically deploy to the Vehicle MEC any intermediate components until the cloud, thus offering a flexible end-to-end 5G connectivity. That is there should be in place an established control path connection that allows the vehicle MEC to be remotely controlled and provisioned and a data path that is used (by deployed VNFs) while in operation to monitor and store vehicle’s data in the cloud. Section 3 presents how this is implemented with VNF and NSD provisioned through OSM.

* + 1. *Assisted Overtaking*

In this scenario, each vehicle consists of an OBU that provides a communication bridge between vehicle and vehicle and infrastructure. The OBU connects to any applications like Android devices, smartphones, etc. which provides visual information for the driver. The vehicle is assisted with front and back cameras which will guide the driver to make a decision, whether to overtake or not. Two VNFs are developed: video transcoding and cellular gateway VNFs. The multi-technology communications support is explored in several experimental situations

In the first one, the video is streamed from the front vehicle to the rear vehicle through the vehicle to vehicle communications, using IEEE 802.11p communication. The OBU in the car receives the video stream and sends it to the visual screen in the car so that the driver can have real-time access to the visual information of the vehicle. This situation requires the VNF video transcoding to be implemented in the cars since the video transmission is performed horizontally between the vehicles.

In the second one, the front and rear cars are in the range of roadside units (RSUs), and the video is streamed to the VNF video transcoding at the edge through the RSUs to reach the rear car. Finally, cars and RSUs are not in the range of each other, and the video is streamed to the VNF video transcoding at the edge of the network using a 4G/5G network to communicate between the cars and the edge network. The 4G/5G network is made available through a VNF Gateway. In this case, it is possible to use the VNF video transcoding from the front car to the rear car by traversing the Cloud-Ran at the edge of the infrastructure.



# Fig. 4.2 Architecture for Assisted overtaking

**CONCLUSION:** In this paper, we survey the literature on security of cyber-physical systems, with a special focus on representative CPS applications: The Remote Monitering Vehicle and the Assisted overtaking . We also present a cyber-physical security framework that incorporates CPS aspects into the security aspects. The framework captures how Cellular Network can be connect the vertical domains of a CPS. This can result in unexpected consequences in the cyber domain and vice versa along with proposed solutions. Implementing the cellular network in CPS can help in the defense academy or services to guide them from the attacks from the enemies. Even for the society Network based CPS helps in assisting the traffic and remote sensing for the physical systems.

# REFERENCES:

1. B. Craggs and A. Rashid, "Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design," *2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, Buenos Aires, 2017, pp. 22-25.
2. R. Atat, L. Liu, H. Chen, J. Wu, H. Li and Y. Yi, "Enabling cyber-physical communication in 5G cellular networks: challenges, spatial spectrum sensing, and cyber-security," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 1, pp. 49-54, 4 2017
3. H. Guo and J. W. Wong, "Cyber-physical authentication for metro systems," *2017 23rd Asia-Pacific Conference on Communications (APCC)*, Perth, WA, 2017, pp. 1-6
4. Behrad Bagheri, “Big Future for Cyber Physical Manufacturing Systems” by, NSF1/UCRC for Intelligence Maintenance Systems(IMS) and JAYLEE, University of Cincinatti.
5. J. M. Taylor and H. R. Sharif, "Security challenges and methods for protecting critical infrastructure cyber- physical systems," *2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, Avignon, 2017, pp. 1-6.
6. S. Li, Q. Ni, Y. Sun, G. Min and S. Al-Rubaye, "Energy-Efficient Resource Allocation for Industrial Cyber- Physical IoT Systems in 5G Era," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2618-2628, June 2018.
7. R. Atat, L. Liu, H. Chen, J. Wu, H. Li and Y. Yi, "Enabling cyber-physical communication in 5G cellular networks: challenges, spatial spectrum sensing, and cyber-security," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 1, pp. 49-54, 4 2017
8. C. Tranoris, S. Denazis, L. Guardalben, J. Pereira and S. Sargento, "Enabling Cyber-Physical Systems for 5G Networking: A Case Study on the Automotive Vertical Domain," *2018 IEEE/ACM 4th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, Gothenburg, Sweden, 2018, pp. 37-40.

[9] B.Craggs and A. Rashid, "Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design," *2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, Buenos Aires, 2017, pp. 22-25.

[10] H Guo and J. W. Wong, "Cyber-physical authentication for metro systems," 2017 23rd Asia-Pacific Conference on Communications (APCC), Perth, WA, 2017, pp. 1-6.

[11] R. Altawy and A. M. Youssef, "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices," in IEEE Access, vol. 4, pp. 959-979, 2016.