Safety and Security of Cyber-Physical System: A Security Framework

Author

Shahbaz Ali Imran

Registration Number

01-241171-037

Supervisor

Dr. Sabina Akhtar

A thesis submitted to the Department of Software Engineering, Faculty of Engineering Sciences, Bahria University, Islamabad in the partial fulfillment of the requirements of a Master degree in Software Engineering

September 2019

Abstract

Although, we have seen rapid growth in the study, development and deployment of Cyber-Physical System in past decades. However, security threats are always there and numbers of security threats have also been improved, but numbers of new vulnerabilities, new kinds of attacks and different system's compromising injections demand to explore more about CPSs in the light of security [2, 4]. In this research, we discuss about the safety and security of Cyber-Physical Systems and secure the communication of CPS using MQTT protocol. For consistency we will now use the term 'CPS' instead of Cyber-Physical System. We have used a water supply SCADA system to simulate the proposed framework about the safety and security of Cyber-Physical System. We have introduced liveness in our proposed framework to confirm that the triggered message has reached to its destination without any packet loss. As its development is not that easy, so for development, we have used NODE-RED a simulation tool to simulate our security framework and for language we have used NODE-JS. As the structure of CPS is very critical, so we have designed the flow of its communication we placed two CPS at two different places, which transfers the water from well to different tanks. The transfer of water flow is triggered through MQTT protocol and then check the accuracy of our proposed framework. This security framework of CPS is immune to all kinds of cyber-attacks due to its liveness property. Different secure ports have a major role in this development. We have also used LOIC to check the immunity of our proposed framework.

Key Words: CPSs, Safety, Security, Cyber security, MQTT, Liveness

Dedication

Dedicated to my exceptional parents and adored siblings whose tremendous support and cooperation led me to this wonderful accomplishment.

Acknowledgements

I am grateful to my creator ALLAH Subhana-Watala to have guided me all through this work and for incorporating new ideas in my brain and giving me the capability to deliver my project. In reality, I could have done nothing without your precious help and direction. Whosoever helped me over the span of my proposition, regardless of whether my folks or some other individual was Your will, so in reality none be deserving of recognition however You.

I would like to thank my thesis advisor, Dr. Sabina Akhtar from BUIC (CS Department). The door to Dr.Sabina office was always open whenever I ran into a trouble spot or had a question about my research or writing. She consistently allowed this research to be my own work, but steered me in the right the direction whenever I needed it.

I am lavishly grateful to my beloved parents who raised me, I was not fit for strolling and kept on supporting me all through in each branch of my life.

At last, I might want to offer my thanks to everyone who have rendered profitable help to my study.

Contents

List of Figures

Chapter 1

Introduction

We have seen a rapid growth in the study, developments and deployments of Cyber-Physical systems during the past years [3]. CPSs are integrated of computations, organizing, and physical procedures. PCs and embedded monitoring and the control of physical procedures, with feedback loops where the procedures of physical affect the calculations and vice-versa. For consistency from now on will use the term “CPS” instead of cyber physical system [1]. Software/ hardware systems and components are working together over a network; their combination defines the concept of CPS [2]. Examples of CPSs are atomic reactors, smart grids, robotics systems, autonomous automobiles (Smart-Cars) etc. Systems like smart grids, electrical power supply, transportation systems, household appliances and healthcare devices, etc. have the critical infrastructure so they are assumed to be that they are not vulnerable and are immune from all kinds of attacks, which is actually not possible in the real-world [3]. In this research our main task is to develop a framework for CPS that is safe and secure. We develop a framework that is immune to all kinds of attacks.

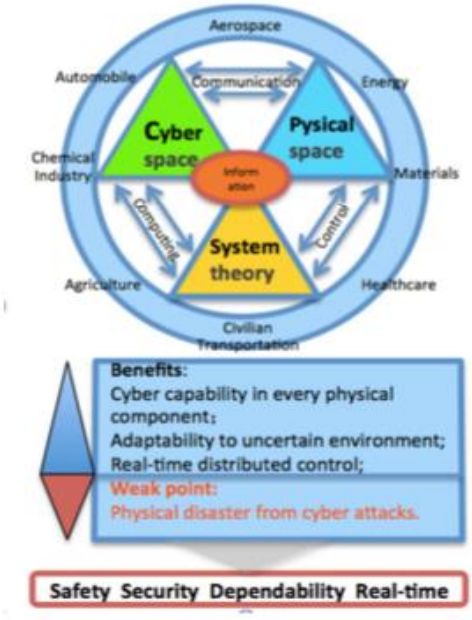

Figure 1: Conceptual model of CPS [2]

The main problem in CPS is the heterogeneity. As CPS is the collection of different components, different hardware components, e.g. embedded systems, sensors and actuators, etc. In the same software different components are used for controlling and monitoring the end result of this is that every component and their integration can contribute a major part in the attack. For better understanding of the CPS current system and severity of attacks and how to protect the system with this kind of attacks can be very helpful to develop a secure system. Hence, we must be capable of identifying the restrictions or defined limits of CPSs that they should point out towards various kinds of attacks and invent ways to safeguard through those attacks. Well the main problem in CPS is its complicity in the structure and heterogeneity of its components. Due to this (Heterogeneity) behavior many security, privacy and protection's threats have been introduced. With that much complexity of cyber-physical interactions, dangerous kind of loopholes, vulnerabilities and threats have now become hard to handle, furthermore latest kind of issues of security have emerged which are hard to examine and these attacks are untraceable. Extensive knowledge and understandings of cyber-attacks, threats and vulnerabilities is importantly needed for the development of defense mechanism. The study of current security of CPS and controls that are private will also take us to point out the loopholes and new research related aspects [3]. In this research, we developed our own new safe and secure framework for CPSs using Liveness.

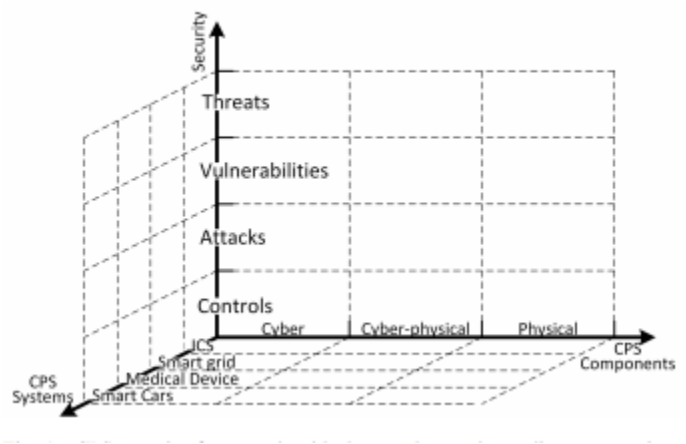

Figure 2: *CPS security framework with three orthogonal coordinates: security, CPS components, and representative CPS systems. [3]*

In this MS research work, we have proposed safety and security framework for CPSs. For communication we have used MQTT protocol. Based on pub/sub or publish/subscribe phenomenon. MQTT protocol works on the top of the TCP/IP protocol. MQTT is a lightweight protocol. The publish/subscribe communication model of MQTT offers a lot of benefits over a traditional pullover response model. We have discussed MQTT in detail in chapter 4.

- ✓ Publish/subscribe
  - Publish information on different devices from your own device and subscribe a specific topic.
- ✓ Messages
  - The type of information exchanged between multiple devices. The information can be data or command.
- ✓ Topics
  - The ways you raise the interest for incoming messages or how we specify the desired location to publish the messages. Strings are the representation of Topic separated by slashes"/".
- ✓ Broker
  - The broker is responsible for receiving all the messages, filtering them and then publishes the message to all the clients which are subscribed.

The third main concept in safety and security of CPS is "Liveness". Liveness refers that "the sent message will be received by the receiver without any packet loss or deadlock".

1.1 Problem Statement

The main problem with the current frameworks in CPS is the safety and security of CPSs, more research work is needed in this regard. Since CPS is a mixture of tightly coupled components therefore security and safety of each component is necessary. There are various frameworks that are Working in the security of CPSs. It is a complex task which also requires domain expertise to relate different security facts with each other on a conceptual level. As the performance of cyber attacks is increasing day by day. So our security parameters should be capable to survive or fight against those attacks without any loss or damage.

1.2 Proposed Research Framework

This research thesis proposes a novel methodology for safety and security of CPS dependent on MQTT and Liveness phenomenon. The proposed safety and security framework of CPS is based on a SCADA system on which we implement our desired techniques. The example we used is of a water company which have two tanks and two pumps, first pump pulls out the water and transfer it to pump 1 and the second pump pulls the water from tank 1 and transfers it to tank 2 which is placed in the different city.

We have used MQTT protocol for starting and stopping the water transfer system. When the water level is below from the certain level the liveness phenomenon gets triggered and it automatically fills the tank to the desired level. The proposed framework is developed in Node-Red (Alter the complex water SCADA system). The alarm was already set. Let's say that Pump 1 and tank 2 are assumed to be two CPS according to our safety and security framework of CPS. The communication from the pump 1 to tank 2 is done by the MQTT protocol for safety; we have used secure ports for MQTT, meaning the start/stop phenomena based on MQTT protocol.

When the run button is in start state the transfer of water will start by pump 1 (Well) and transfer the water to tank 1 and tank 1 will transfer to the next pump and pump 2 will transfer the water to tank 2.

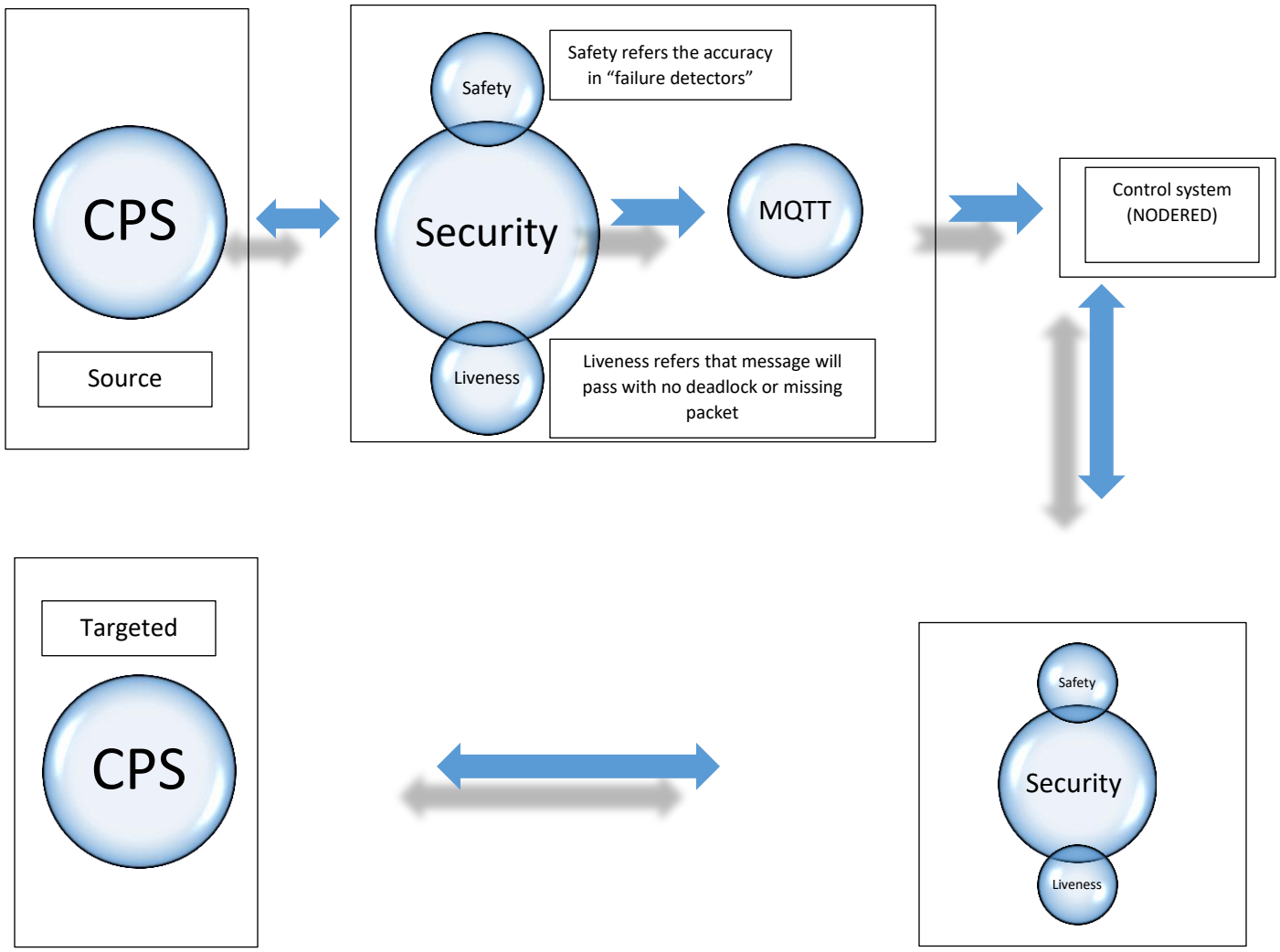

Figure 3: *CPS security proposed framework*

1.3 Structure of the Thesis

The rest of the thesis is organized in a manner where Chapter 2 describes the background and the related work. Chapter 3 explains the methodlogy and motivation behind the proposed technique and Chapter 4 describes the Implementation in detail. In, Chapter 5 experimental results are presented. Finally, Chapter 6 concludes our thesis.

Chapter 2

Background and Related Work

This section provides a brief background of safety and security of CPS.

2.1 Related Work of Safety and Security of CPSs

Sr#	Title	Authors	Objective	Year	Conclusion
1.	CPSs Security—A Survey	Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo	A survey of the security of CPSs	Dec-2017	Extract the knowledge from previous frameworks and research Papers.
2.	An Effective Security Requirements Engineering Framework for CPSs	An Effective Security Requirements Engineering Framework for CPSs	Gathered the Security requirements for the CPS.	JUL-2018	They have gathered the requirements of security for CPSs that lead them to cross the boundaries of the domain of Software engineering to secure the CPS.
3.	A Security and Safety Framework for Cyber Physical System	Peiyuan Dong, Yue Han, Xiaobo Guo , Feng Xie	To develop a security framework for CPSs.	Jan-2015	For cyber they have used Opennet++ and for physical components, they

					used Matlab and PLC
4.	An Efficient MQTT Framework for Control and Protection of Networked CPSs	Utku Ozgur, Harikrishnan T. Nair, Aditya Sundararajan, Kemal Akkaya and Arif I. Sarwat	To develop a security framework for CPSs.	Oct-2017	Placed two CPS in two different places and check the message integrity in the form of charts using MQTT protocol and the Arduino controller in hardware loop the whole system develop in MATLAB
5.	Systems engineering framework for cyber physical security and resilience	Zachary A. Collie, Igor Linkov, Daniel DiMase, Kenneth Heffner	Security framework for CPS	Feb-2015	Uses SEP approach and develop a lexicon tat are specific to CPS security to assess the health issues
6.	A multi-layered and kill-chain based security analysis framework for CPSs	Adam Hahn , Roshan K. Thomas , Ivan Lozano , Alvaro Cardenas	Analyses the attacks on CPS	Aug-2015	They have done the groundwork for a framework to analyse the attacks. Successfully implementing attacks on CPS to check how the

					physical layers and components related to cyber layer and controls and affect their selves or each-other.
7.	Towards a Framework for Assuring Cyber Physical System Security	Tianbo Lu, Jinyang Zhao , Lingling Zhao , Yang Li and Xiaoyan Zhang	CPS security framework review for better understandings of CPS vulnerabilities	Sep-2015	Survey various universities and institutes that are related to CPS research, to achieve knowledge of CPS security in different aspects and learn different approaches towards security.
8.	Security framework for industrial collaborative robotic CPSs	Azfar Khalid, Pierre Kirisci, Zeashan Hameed Khan , Zied Ghrairi , Klaus-Dieter Thoben , Jürgen Pannek	Security framework for ROBOT – HUMAN collaboration in the leaf CPS industry	Feb-2018	Explain a secure robotic CPS collaboration and cyber-attacks in the light of Collaborative CPS.
9.	A survey on security control and attack detection for industrial CPSs	Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang	Security and attack detection of CPS	Oct-2017	Overview of recent CPS security parameters and detection of cyber-attacks, they have also discussed

					robustness and stability were also discussed to check the weakness of cyber attacks
10.	Standardization in CPSs: The ARUM Case	Paulo Leitão, José Barbosa1 , Maria-Eleftheria Ch. Papadopoulou , Iakovos S. Venieris	Security of CPS in the light of ARUM projects	Mar-2015	Current requirements that impose the CPS to its limitation, standards are also discussed development of standard-compliant service-oriented multiagent systems in the circle of the solution of ARUM project
11.	Cyber-Physical-Security Framework for Building Energy Management System	Kaveh Paridari, Alie El-Din Mady, Silvio La Porta, Rohan Chabukswar Jacobo Blanco, André Teixeira, Henrik Sandberg, Menouer Boubekeur	Build a cyber-security framework for energy management system	Apr-2016	Presented a framework which uses a mechanism of physics to ~~which~~ derive the security information. They have tested the frequency of framework by implementing a real critical attack.
12.	CPSs, internet of things and big	Sergio F. Ochoa , Giancarlo	Introduces the issues in IOT,	Dec-2015	Read different articles to know the

	data	Fortino , Giuseppe Di Fatta	CPS and Big Data as these three fields are of interest in this era and for future perspective.		loopholes and issue in the field of IOT, CPS and Big data
13.	Cross-Domain Security of CPSs	Sujit Rokka Chhetri, Jiang Wan, Mohammad Abdullah Al Faruque	Cross domain security implementation /analysis of CPS	Jan-2017	They have manufactured a framework which is used as a study. Practical analysis of a cross domain framework of CPS, the energy flow of information on CPS.
14.	The Security Challenges in the IoT enabled CPSsand Opportunities for Evolutionary Computing & Other Computational Intelligence	Hongmei He, Carsten Maple , Tim Watson , Ashutosh Tiwari, Jorn Mehnen , Yaochu Jin , Bogdan Gabrys	An overview of security challenges faced in IOT enabled CPS field and research guidance	Jul-2016	Survey based research paper for security challenges in IOT
15.	A Security Architecture in CPSs: Security Theories,	Riham Altawy And Amr M. Youssef,	A survey of the security of Cyber Physical system.	Jan-2016	Survey based research. They have analysed the current security

	Analysis, Simulation and Application Fields		For medical devices		parameters and proposed solution and then check the strengths and limits of proposed solutions.
16	A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive CPSs	Christoph Schmittner, Zhendong Ma, Erwin Schoitsch, Thomas Gruber	Identify the security breaches by comparing Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) and Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS)	Apr-2015	This paper demonstrates a contextual investigation of applying Two promising examinations Strategies (FMVEA and CHASSIS) to automotive CPS
17.	Secure CPSs: Current Trends, Tools and Open Research Problems	Anupam Chattopadhyay, Alok Prakash, and Muhammad Shafique	Securing CPS by best Understanding of cyber-attacks and check the inadequacy of current security tools	May-2017	This paper introduced a diagram of cutting edge secure CPS plan and execution, including ongoing patterns and apparatuses to

					battle the constantly developing dangers
18.	A Conceptual Framework for Modelling and Design of CPSs	Ioan Dumitrache , Ioan Stefan Sacala, Mihnea Alexandru Moisescu , Simona Iuliana Caramihai	A Conceptual security framework for CPS	Sep-2017	A simple or Generic architecture which is based on CPS, the idea has been proposed utilizing a predefined situation
19.	CPSs Security: a Systematic Mapping Study	Yuriy Zacchia Lun , Alessandro D'Innocenzo , Ivano Malavolta , Maria Domenica Di Benedetto	Analyse and identify the current studies on the security of CPS, and point out the security concerns of CPS	May-2016	Analyze the existing techniques for the security of CPS from the point of view of researchers.
20.	A Survey on Smart Grid Cyber-Physical System Testbeds	Mehmet H. Cintuglu,Osama A. Mohammed, Kemal Akkaya,A. Selcuk Uluagac,	Survey on CPS security	Nov-2016	Survey of CPS security in four steps,first communication infrastructure, smart grid fields, test platforms and research goals
21	On modelling of electrical CPSs considering	Yi-nan Wang Zhi-yun Lin	Security Framework for ECPS(Electrical	May-2016	Introduce a new framework for ECPS. Different

	cyber security	Xiao Liang Wen-yuan Xu Qiang Yang Gang-feng Yan	cyber physical systems)		types of channels related to information (Information channels) which characterized the dependency of interconnected based on network
22.	Smart Grids: A Cyber–Physical Systems Perspective	Xinghuo Yu ; Yusheng Xue	Understanding of CPS in the field of smart grids	Mar-2015	Discuss the contribution of CPS in SGs
23.	Towards a Framework for Assuring Cyber Physical System Security	Tianbo Lu , Jinyang Zhao , Lingling Zhao , Yang Li1 and Xiaoyan Zhang	Framework for the security of CPS	Mar-2015	Introduce a new security framework for CPS. By analyzing different Universities research works in the field of CPS security .but also define three levels
24.	On Bounded Rationality in CPSs Security: Game-Theoretic Analysis with Application to Smart Grid Protection	Anibal Sanjab and Walid Saad	Protection of Smart grids	Oct-2016	A game theoretic approach is used to demonstrate the attacker and defender activities which define the protection of smart grids.

25.	Smart Human Security Framework Using Internet of Things, Cloud and Fog Computing	Vivek Kumar Sehgal, Anubhav Patrick, Ashutosh Soni and Lucky Rajput	Security related decision using fog,cloude and IOT	2015	Introduce Security framework using IOT, Cloud and FOG.

For the better understanding of CPSs we have gone through previous studies as CPSs and their vulnerabilities are well-studied area in recent years; an ample work of research has been done in the area of safety and security of CPSs. Utku Ozgur and Harikishan T. Nair with their companion has introduced their own framework for the safety and security for CPS.They have named their framework as an “NCPS TESTBED” and their setup consists of two identical hardware’s which are placed in two different cities. One is located in Miami, Florida and the other one is in Philadelphia.They have passed real time information between these two identical servers using MQTT protocol to check their framework. The authors of this paper have also discussed three types of attacks.

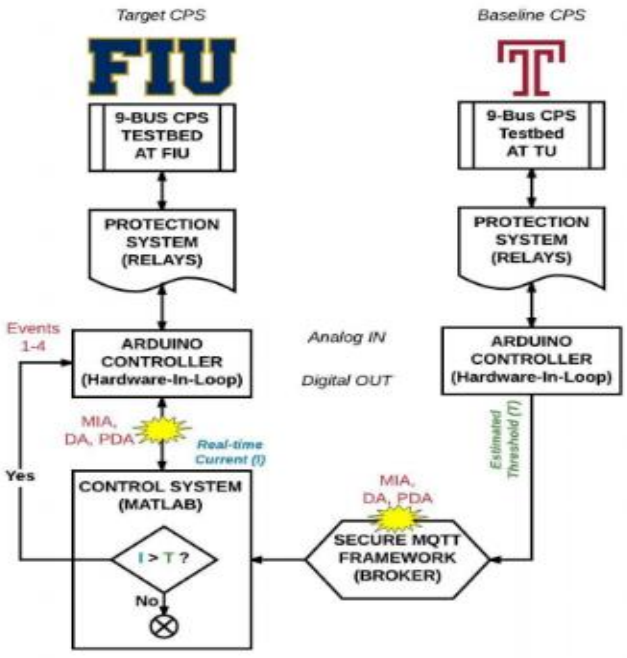

Figure 4: *The NCPS Test bed Setup and the Attack Model Considered.[5]*

One is Message integrity attack (MIA), the second is a Delay attack (DA) and the third is Packet drop attack (PDA) that are also shown in their proposed framework image mentioned below [4].

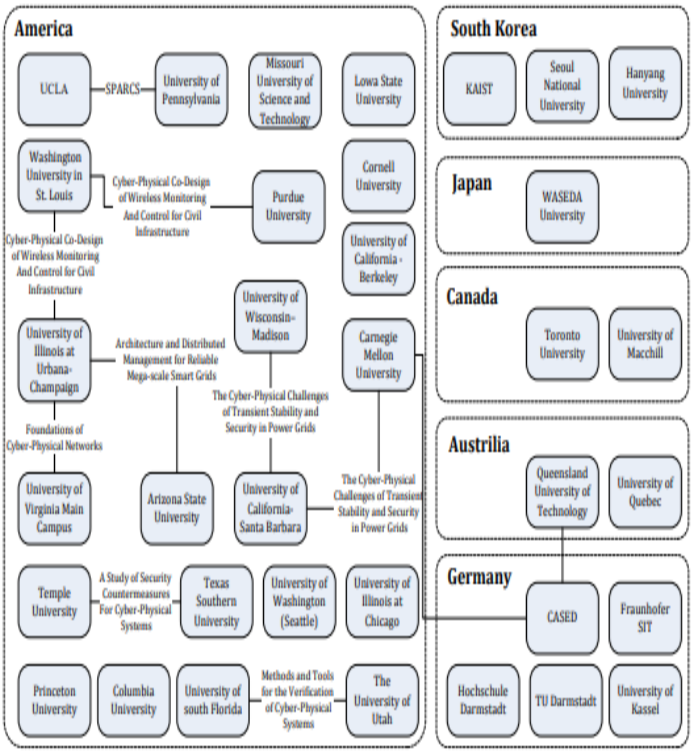

Figure 5: *Universities Studying Security of CPS and their Relations [7].*

This article gives an extensive audit of CPS security following the security structure from different points of view. With the expanding common use and vulnerabilities of CPS to cyber-physical attacks, CPS security is assuming a fundamentally significant job in the examination of CPS. They have overview the primary colleges and foundations driving the exploration of CPS security and examine their examination centers and the relations between them [8].

The targets for accomplishing security of CPS in various angles are presented with related writing efforts. Then the fundamental security approaches to recognizing cyber-physical attacks and guaranteeing CPS security are recorded and broke down. At last, they rundown security in explicit applications with the predominant research bunches presented. As a consequence of their endeavors, it is seen that security research is a long way from full grown for the recently rose cyber physical systems and there are numerous difficulties confronting architects, administrators and specialists. This is unacceptable, and ideally, by giving an outline of the writing endeavors done, the review will contribute

in giving a reference to a specialist in the territory of CPS security. Their framework figure is mentioned below.

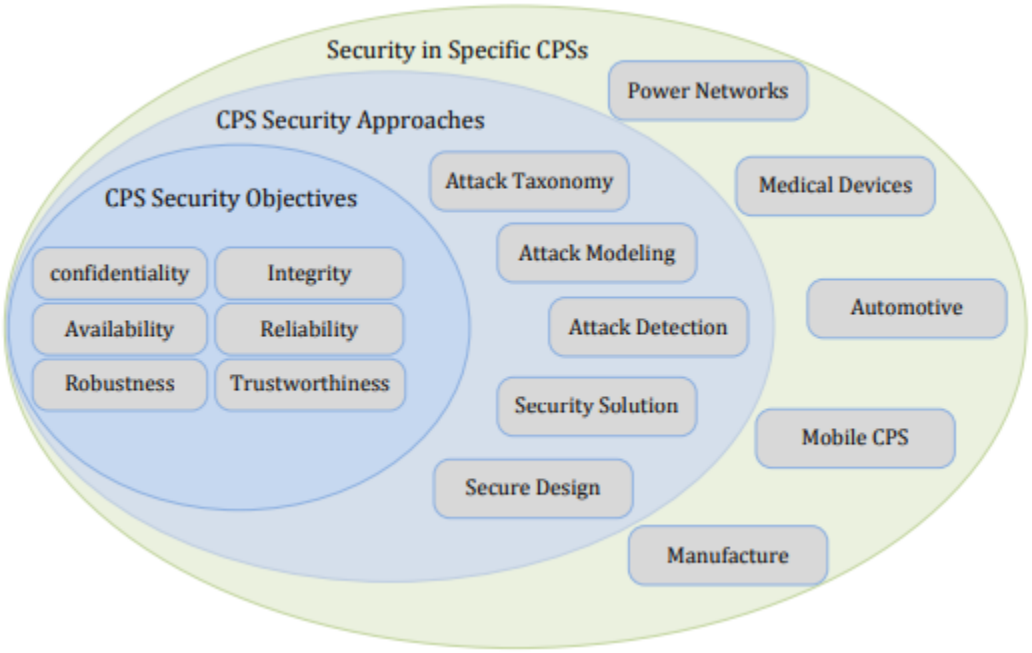

Figure 6: *Security Framework of CPS proposed by Mr.lu and Mr.Li [7]*

In another survey on the security of CPS the author studied CPS, which will cover different parts of social and financial life and how they bring a wide impact and lead the complete improvement of software engineering just as different subjects. However, limited by the current hypothesis and innovation of calculation, correspondences and control innovation, the advancement of CPS likewise confronts enormous difficulties. Leap forward in CPS key innovation will empower our nation to take the world's driving position in the CPS advancement so they can freely set their own standard and to push the national social and financial improvement [8].

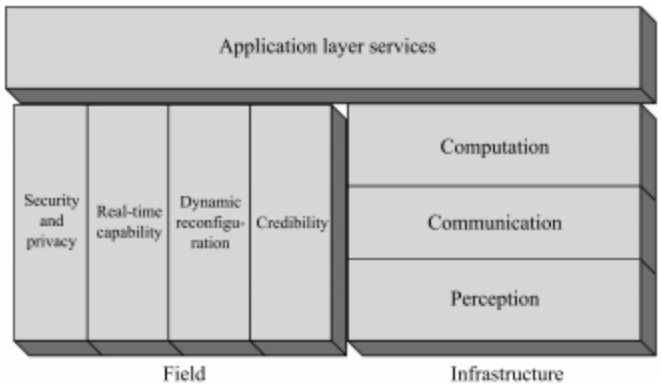

Figure 7: *CPS Integration [8]*

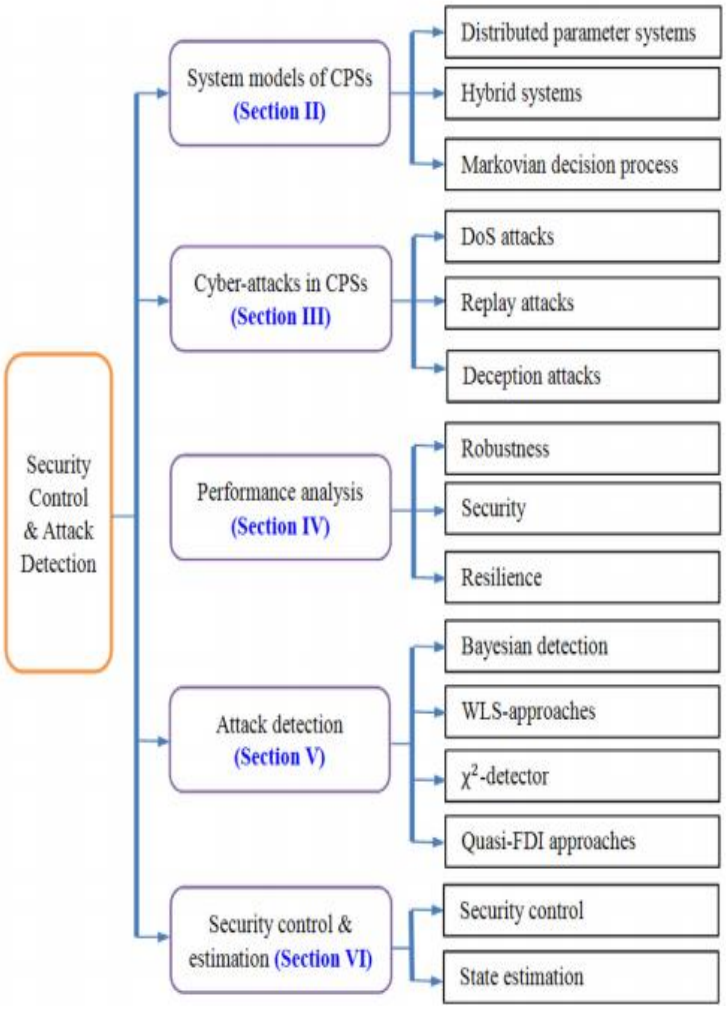

Figure 8: *Research's survey structure [10]*

The paper written by Kaveh paridari with his colleagues about the CPS framework of energy management system, that paper presented a cyber-security structure as relevant to a structure Energy Management System. The structure uses the material study of the system to drive the security information assessment and flexible methodology. The system viability was displayed on an authentic fundamental assault circumstance, where the security information assessment, count triggers the solid control to recover from the assault. Replicating results exhibit that the proposed solid control technique can recover the system from non ordinary conditions, in any case, when there is any existence of a delay for the assault area [12].

This paper presents the unique issue on CPSs, Internet of Things and Big Data. These three interweaves ideas are engaged with the new ages of community-oriented arrangements; especially, in those thinking about gadgets heterogeneity furthermore, specially appointed associations. The examination network has perceived the intricacy of structuring and executing these systems, and likewise, preparing the enormous measure of information they produce. To Contribute address these difficulties, they have chosen ten articles that add to propel the present information in a few angles identified with the structure, execution, and utilization of IoT-empowered CPS [13].

CPSs solidly facilitates physical methodology and information and correspondence headways. As the present fundamental structures, e.g., the power lattice or water allotment systems are astounding CPSs, ensuring their prosperity and security happens to indispensable connote. Traditional prosperity assessment procedures, for instance, HAZOP, are ill-suited to assess these systems. Furthermore, cyber-security vulnerabilities are consistently not contemplated essential, in light of the way that their effects on the physical methods are not totally grasped. In this work, they have shown STPA-Safe Sec, a novel examination system for both prosperity and security. Its results show the conditions between cyber-security vulnerabilities and system prosperity. Using this information, the best alleviation procedures to ensure the prosperity and security of the

system can be immediately perceived. They have associated STPA-Safe Sec as a use case in the power matrix territory, and highlight its focal points [14].

The combination of cyber correspondences and control systems into the power grid foundation is far-reaching and that profoundly affects the activity, dependability, and productivity of the grid [16]. Cyber advances take into consideration the effective administration of the power system, one significant conceivable outcome is the presentation of cyber-initiated or cyber-empowered disturbances of physical segments. In this research, they've proposed an on the web system for evaluating the operational dependability impacts because of dangers to the cyber infrastructure. This structure is a significant advance towards tending to the basic test of comprehension and examining complex CPSs at scale [16].

To comprehend and distinguish the attack surfaces of a Cyber-Physical System (CPS) is a fundamental advance towards guaranteeing its security [21]. The developing unpredictability of the cybernetics and the communication of autonomous spaces, for example, flight, apply autonomy and car is a noteworthy impediment against an all-encompassing perspective CPS. Moreover, the multiplication of correspondence systems has broadened the scope of CPS from a client-driven single stage of a generally disseminated system, regularly interfacing with basic framework, e.g., through keen vital activity. In this composition, they think about this point of view and give an audit of current security patterns and instruments for secure CPS. They stress on both the structure and execution streams and especially feature, the need for proficient attack surface [21].

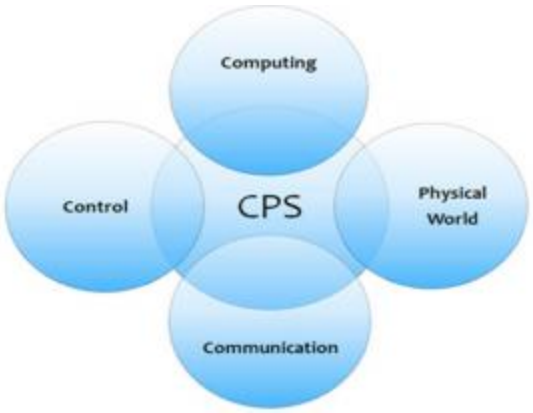

Figure 9: *multidisciplinary view of CPS [22]*

A generic architecture based on CPS idea has been proposed utilizing a predefined situation. A keen homestead can be executed by coordinating the most significant consequences of the exploration in cutting edge innovative fields. Along these lines, CPSs assume a significant job, seen from a multidisciplinary viewpoint [22].

In another research paper the author divides his research in a very decent manner and he describes his research like Objective: In this examination, They target distinguishing, grouping, and breaking down existing examination of CPS security so as to more readily see how security is really tended to when managing digital physical systems. In view of this investigation of the best in class, they also target recognizing the suggestions for future research on CPS security [23].

Proposed Method: In request to accomplish this, They structured and led a systematic mapping concentrate to distinguish, order, and look at applicable examinations proposing a method or procedure for digital physical systems security. An examination framework for ordering methods or systems for CPS security has been observationally characterized; recognized significant examinations have been arranged based on distribution slants, their attributes what's more, center, and their approval systems.

Results: They chose an aggregate of 118 essential examinations as a result of the systematic mapping process. From the gathered information they can see that.

(I) Regardless of whether the answers to CPSs security has developed as of late, in the a year ago, they were increasing a forcefully expanding logical enthusiasm over heterogeneous production settings;

(II) The heft of the chips away at security for CPSs is centered around power grids and the methodologies considering attacks on sensors and their assurance totally rule the scene; paying little respect to application field and thought about system segments, every one of the chips away at CPSs security manage attacks, so as to either execute or to balance them, and assembling every one of these investigations gives us the likelihood to arrange the current (digital physical) attack models; it comes as an unexpected that not many papers think about correspondence angles and endeavor to give non-paltry scientific models of the correspondence.

(III) Most progressive and reasonable approval methods have been misused in the power systems, application space, be that as it may, even there a benchmark is as yet absent. Conclusion: The systematic guide of research on CPS security gave here depends on, e.g., fields of application, different systematic parts, that are related to models and calculations, attacks attributes and resistance methodologies. This work introduces a hotly debated issue, significant for both industry what's more, scholarly community [23].

Communication infrastructure is fundamental for the savvy grid. The vast majority of the test bed's center around the correspondence arranged shrewd grid investigates as far as information, correspondence, correspondence conventions, protection and security of correspondence framework. Shrewd grid acknowledgment is rising in all areas including home gadgets, appropriation field gadgets, substation gadgets, and wide-zone control gadgets. The system type is distinctive in every space, just as actualized correspondence conventions [24].

A CPS situation where a noxious specialist does stick attacks on the corresponding channel between a sensor and a remote estimator. They previously viewed as a circumstance where the sensor, what’s more, the attacker fixes their techniques from the earlier. For the situation where the sensor and the attacker have on-line data about

the past transmission results and the event of attacks, they have given a calculation which plays out the game progressively. They likewise presented an election issue detailing which considers normal vitality imperatives. By utilizing a Markov chain model, they got a closed-form articulation for the objective capacity. The related improvement issue requires altogether less calculation. Potential augmentations incorporate examining the multi-sensor case with obstructions between every sensor and attack from the attacker, and different sort of attacks, including trickiness attack, which spotlights on the honesty of the information by adjusting the information parcels [25].

Another framework for ECPSs [26], where a correspondence system and its relationship are structured by the attributes of a given power grid. Specifically, they have described the interdependency of associated systems dependent on various sorts of data channels. Control techniques, for example, load shedding and hand-off insurance and attack situations have additionally been connected to the planned correspondence systems for examining falling disappointment spread [26].

In another study in the field of CPS the author describes that Smart grids are electrical systems that utilize propelled observing, control, and correspondence innovations to convey solid and secure vitality supply, enhance operational productivity for generators and wholesalers, and give adaptable decisions to presumes. Shrewd grids are a blend of complex physical systems and digital systems that face numerous innovative difficulties. In this paper, first, they have introduced an outline of these difficulties with regards to CPSs. At that point they lay out potential commitments that CPSs can make to shrewd grids, just as the difficulties the savvy grids present to CPSs [27].

CPSs are getting more well known in power systems, social insurance gadgets, transportation systems, mechanical procedure, and frameworks. As CPSs are utilized increasingly more widely and completely, the security parameters of CPS have now turned into almost extreme significant worry in system structure, usage, and research. Numerous sorts of attacks emerge (for example the Stuxnet worm), causing substantial misfortunes and genuine potential security dangers. For the couple of

years till now, analysts are concentrating their looks into on changed security parameters chunks for CPSs. According to this research paper [28], they have proposed a framework of security and guaranteeing the security of CPSs and dissect primary colleges and foundations contemplating CPS as the relation of its components and security in three levels: objectives, approaches and outside applications in the security shelter for CPSs [28].

Vivek Kumar Sehgal [31], in his research of security has explained that "Mishaps and mechanical events have turned out to be real. PCs and contraptions have advanced a great deal in the early years or decades, however, very little has yet been done to handle difficulty, yet gigantically significant field of security that deals with physical of individual components. Coming with the unavoidable registering, the (IoT), ubiquitous distributed computing and its expansion mist processing, now turned out to be conceivable to give security spread to individuals and upset any offense against them. They have given framework of security that joining inescapable and wearable figuring, IoT, cloud, and fog computing to protect people and block any setback" [31].

2.2 Comparative Analysis Table:

A brief comparative analysis between different papers is presented in the following table.

S#	Year	Authors	Title	Liveness
1	2018	Azfar Khalid, Pierre Kiriscib, Zeashan Hameed Khand, Zied Ghrairic, Klaus-Dieter Thoben, Jürgen Pannekb,	Security framework for industrial collaborative robotic CPSs	No
2	2015	Giedre Sabaliauskaite and Aditya P. Mathur	Aligning Cyber-Physical System Safety and Security	No
3	2015	Adam Hahn, Roshan K. Thomas, Ivan Lozano, Alvaro Cardenas	A multi-layered and kill-chain based security analysis framework for CPSs	No
4	2015	Peiyuan Dong, Yue Han, Xiaobo Guo and Feng Xie	A Systematic Review of Studies on Cyber Physical System Security	No
5	2015	Christoph Schmittner, Zhendong Ma, Erwin Schoitsch, Thomas Gruber	A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive CPSs	No
6	2015	Tianbo Lu, Jinyang Zhao, Lingling Zhao, Yang Li and Xiaoyan Zhang	Towards a Framework for Assuring Cyber Physical System Security	No
7	2016	Ivo Friedberg Kieran McLaughlin PaulSmith David Laverty Sakir Sezer	STPA-SafeSec: Safety and security analysis	No

			for CPSs	
8	2015	Vincenzo De Florio, Giuseppe Primiero	A framework for trustworthiness assessment based on fidelity in cyber and physical domains	No
9	2015	Wojciech Grega, Andrew J. Kornecki	Real-Time CPSs Transatlantic Engineering Curricula Framework	No
10	2014	Peyman Dong, Yue Han, Xiaobo Guo, feng Xie	A security and safety framework for Cyber-Physical system	No
11	2017	Utku Ozgur, Harikrishnan T. Nair, Aditya Sundararajan, Kemal Akkaya and Arif I. Sarwat	An Efficient MQTT Framework for Control and Protection of Networked CPSs	NO

2.3 Base Paper Impletation and comparison

To compare the immunity of our framework we have also implemented the framework that was implemented (without Liveness) on our NODE-RED tool and then applies the DDOS (Distributed denial of service) where results shows that the system got stuck when the attack applied on the framework.

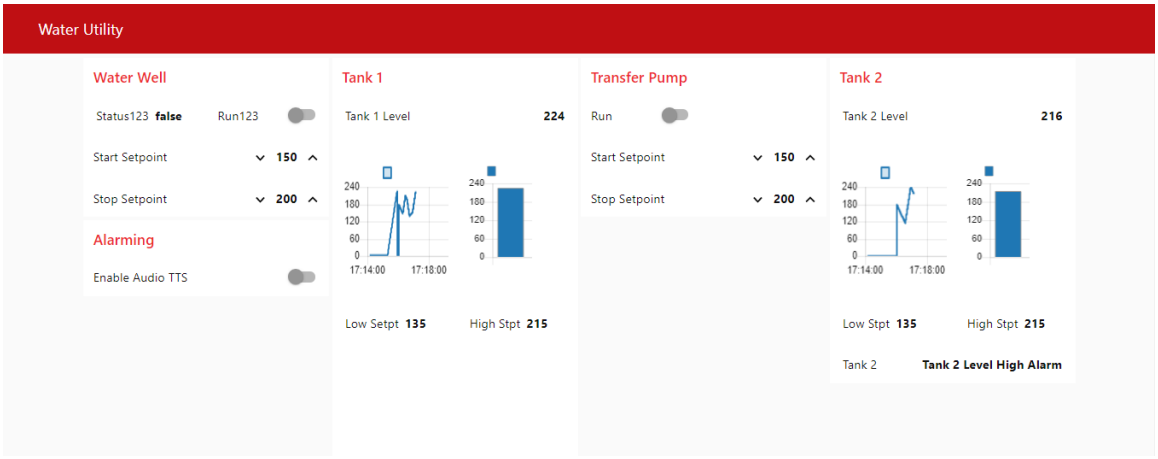

Figure10: *Implementation of the Framework*

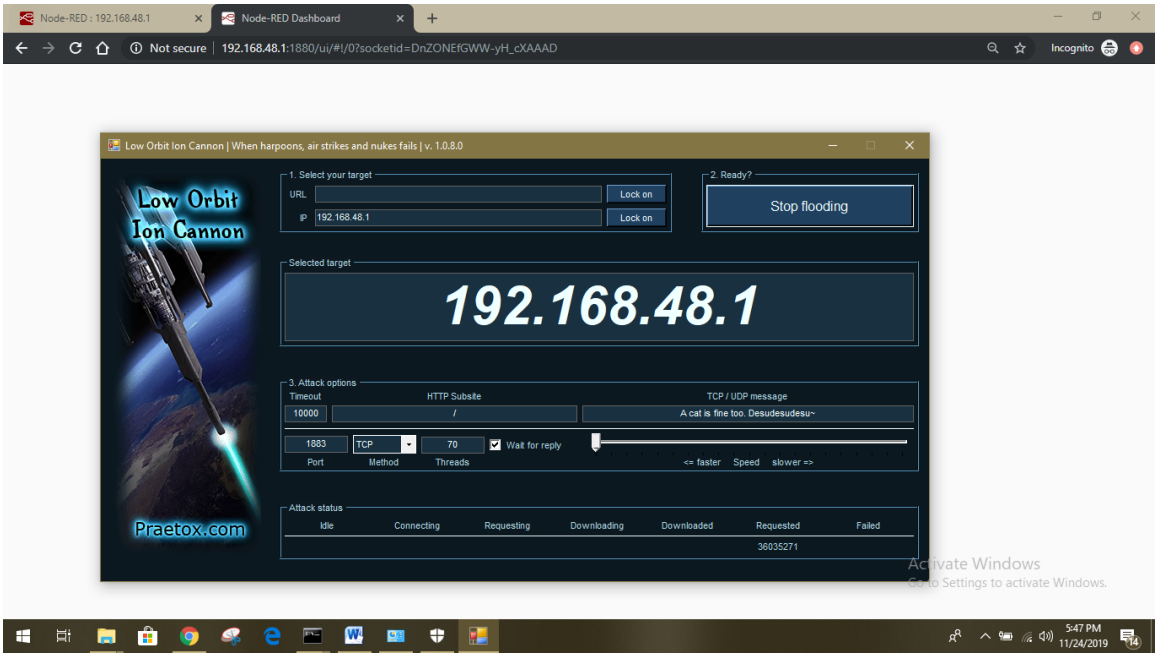

Figure 11: *While appltying DDOS attack Tab 2*

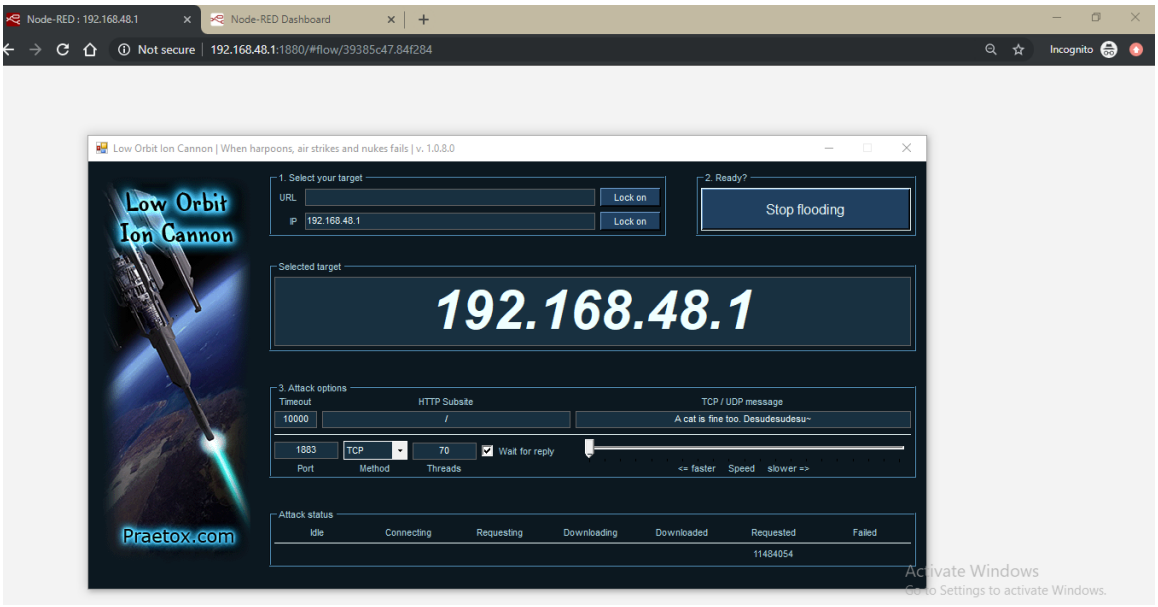

Figure 12: *While appltying DDOS attack Tab 1*

Figure 11 & Figure 12 shows that the system is totally unresponsive. Moreover, both tabs are not responding under DDOS attack.

Chapter 3

Methodology

Overview

This chapter briefly explains the actions that are performed to identify, collect, process and analyze the data to better understand of our research domain.

3.1 Proposed Methodology

The proposed framework is based on the Safety and Security of Cyber Physical Systems. The current frameworks for security of Cyber-Physical Systems somehow limit [2, 4]. The motivation behind the research is to acquire knowledge from the previous frameworks. The knowledge gathered from previous work will now be used to develop the new framework with enhanced features for Cyber Physical Systems. We have incorporated the added feature of liveness in the proposed system which not only help to retain the information in the message, but also give the confirmation that the message was sent successfully without any packet loss. Furthermore, there is no deadlock in the proposed framework. Moreover, we have used MQTT protocol for communication between two CPSs over WAN (Wide Area Network). Another main component is Mosquitto Broker which helps the connectivity of client and server in the MQTT protocol. By using this security, proposed framework will bring a massive improvement in the security of CPS. Another advantage of this framework is the satisfaction that the sent information received by the receiver even in case of cyber attacks.

3.2 Problem Discovery

In any research process, the first step is to discover a problem in a specific area. Therefore, to identify the problem in the specific domain of CPS, a lot of background study was required. After a comprehensive background study, we find out that the problem with the current framework is its incapability to incorporate liveness in a system. So, if the system does not include liveness, then there is no information about the packets. This can be very harmful as the user does not have any information about the system.

3.3 Analysis

In this section, different tools and techniques are explained for the proposed scheme to develop our framework to achieve the desired goal. Node-Red simulation tool was used to make the framework using node-js. This section is divided into 4 parts. The first part is about methodology which briefly explain the working of the proposed. Lately Mr.P.Dong [3], has also proposed a security framework for CPS in Jan-2015. As for cyber they have used Opennet++ and for physical components, he used Matlab and PLC. Similarly Utku Ozgur and Harikrishnan T. Nair in their research work placed two CPS in two different places and check the message integrity in the form of charts using MQTT protocol and Arduino controller. These two papers are discussed because they are the base papers of our research, we have tried to cover the loopholes in all aspects in the field of CPSs.

3.4 Tools for supporting system framework

In this section, different tools and techniques are explained for the proposed scheme. We have used Node-Red programming tool for wiring different hardware devices together. Node Red is a web-based flow editor that is used to create different Java Script functions.furthermore, we have used Node JS for different event driven servers. Node JS cross-platform open source Java Scripts platform, is used for executing Java Script code outside a browser. The Node-JS platform is single threaded in nature used for different websites and backend API's.

3.4.1 Node RED

Node-RED is a tool or platform which is very simple and easy to use. Ready-made programmed components can be used for simulation.

3.4.2 Node JS

An Open-source programming language. Node-js was composed at first by Ryan Dahl in 2009 after the presentation of primary server-side JavaScript condition, Netscape's LiveWire Pro Web. The table below describes different reserved words that are used in our implementation.

Table 5 List of Keywords used in Node JS

Sr. No	Keyword	Description
1	Break	Use to jump-out of the loop
2	Continue	Use to jump over iterations
3	Debugger	Use for Debugging
4	Const	To declare a constant in a function.
5	Return	Use to return a value
6	Synchronized	Use for Asynchronous tasks
7	Var	Use to declare a variable
8	Yield	Use for Iterator Result
9	Throw	Use for user-defined exceptions
10	Switch	To perform different conditions

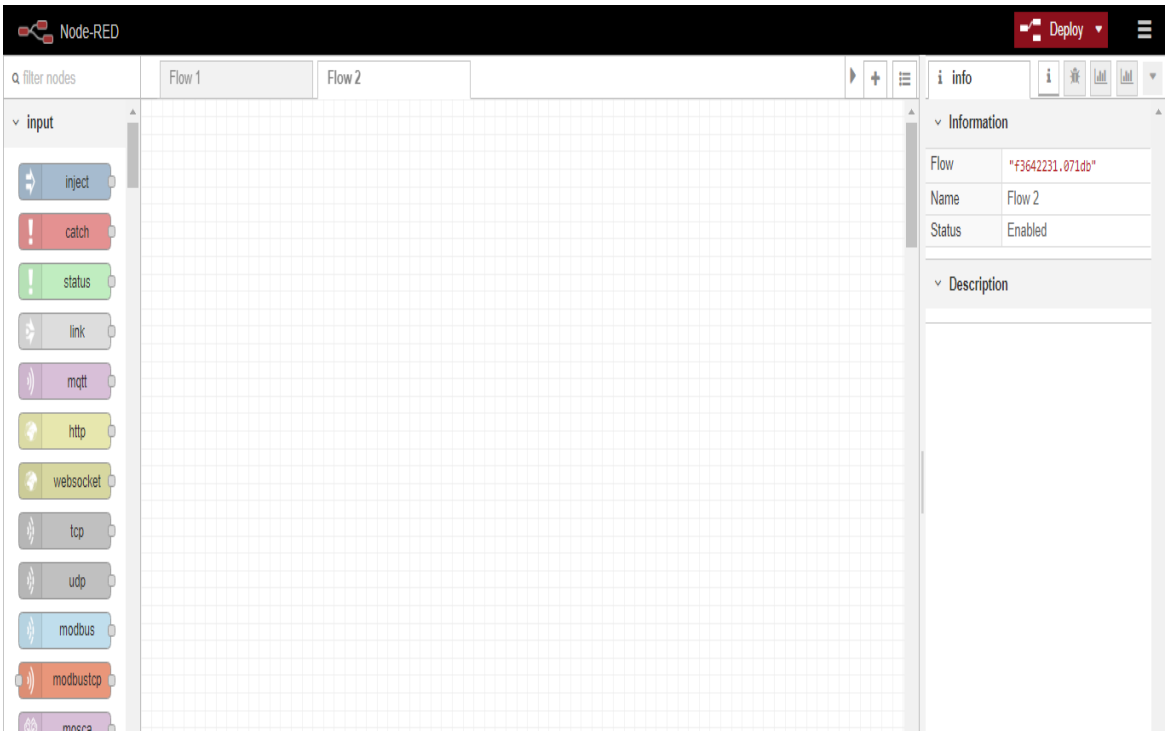

Figure 13: *Basic interface of Node Red*

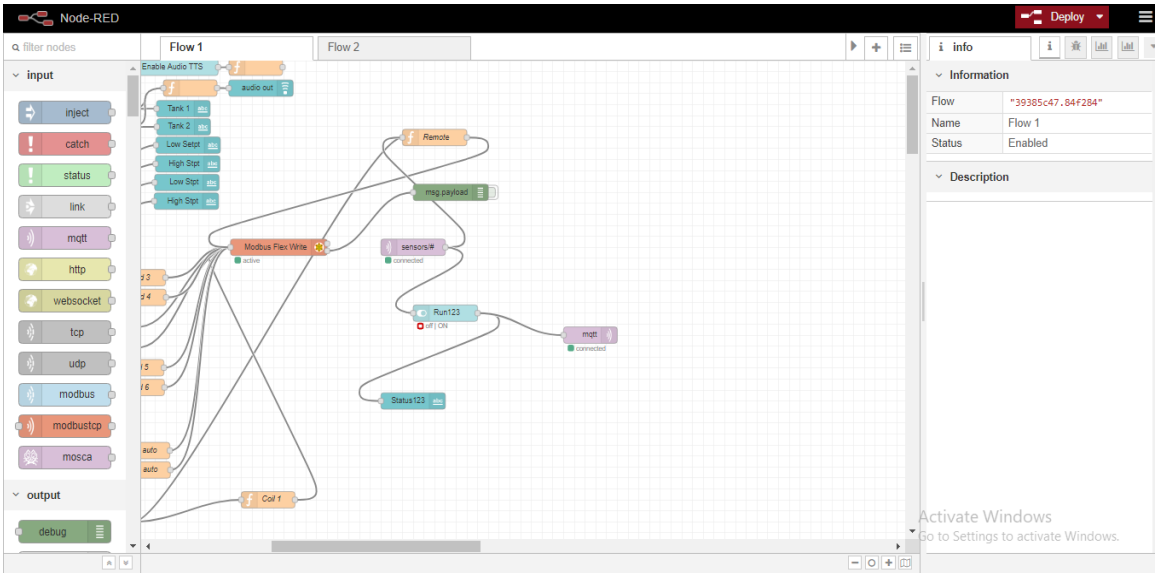

Figure 14: *Basic interface of Node Red*

Chapter 4

Implementation

Overview

This chapter briefly explains the implementation details of our proposed framework. Furthermore, this section will discuss the different phases of the proposed security framework. Moreover, it will discuss the working and the parameters used for security in our proposed framework. Moreover, this chapter will discuss the steps we used to implement our proposed framework.

4.1 Security Framework:

The framework comprises of two pumps and two tanks. The principal pump pulls water from the well in the principal tank, the subsequent pump transfers water from the first to the second tank. This arrangement has four unique areas; every area has a Modbus RTUs or PLCs. The center of this SCADA framework will be Node-Red which will peruse values from the tanks, start and stop pumps, give disturbing, and an HMI.

The Water Well/Transfer pump dashboard values demonstrate the pump mode and status. Tank level set points can be altered to change when the pump in its programming mode consequently starts and stops. In manual mode, the pump can be initialized and halted by hand. The tank values have a line pattern and a bar graph pattern to effortlessly see the level and the history of the level. The alert set focuses are consequently set to be +15 and -15 around the pump start and stop set focuses, this could without much of a stretch be changed to work in an unexpected way. At long last, there is a content alert status that shows if the caution is High, Low, or Clear.

A content to discourse hub likewise declares the caution status. For liveness different check and constraints are used so that it is confirmed that the message will be passed without any interruption. MQTT broker is used on the start button to transfer the pumping of water from a water well. MQTT protocol is used to stop water from the water well by clicking on the stop button. Below figure shows the overall process of the proposed framework.

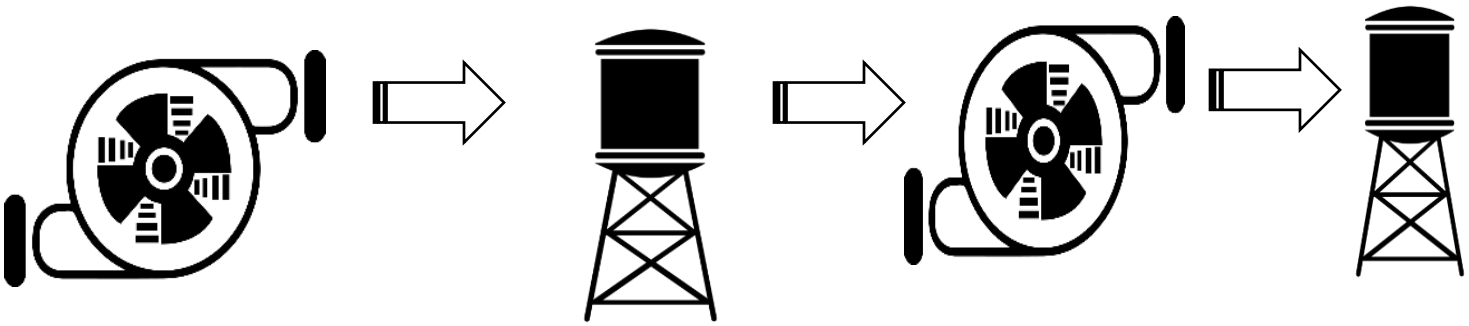

Figure 15: water transfer SCADA system[27]

4.2 Rule Based Approach

We have defined some rules in our proposed framework. There are some thresholds for water level in our system. Our proposed system will send the information non stop unless and until the complete and accurate information will be received by the receiver.

4.3 Development Phases of safety and security of Cyber Physical Systems

In this section, the development phases of our proposed framework are explained. The proposed methodology has six stages which we have explained below;

4.3.1 Source CPS

The first step in developing our security and safety framework is identifying the source for Cyber-Physical System. We have placed one Cyber-Physical System as a source of information. We have not designed the CPS, we have just placed it for starting the flow of information, as the information that is generated from this source will flow through the next nodes, so that there will be no ambiguity in source's authenticity.

4.3.2 Liveness

The second and the most important step of our research is "Liveness". Here Liveness does not mean that we are getting live data. In this case, liveness refers to the Information or message that has triggered from the source CPS, will reach to the destination without any deadlock or packet-loss. This authenticity has a major significance in this type of system, as information is the main aspect.In case the sent message is not received at the receiver end, the whole CPS communication scenario will be in jeopardy. So liveness is

the main aspect of this research by sending the unsent or incomplete message, making it complete and then again send it to the receiver. Liveness is the best contingency plan for this type of communication system.

4.3.3 MQTT Protocol

The other most important aspect of research thesis without which it is difficult to complete the desired safety and security framework is Message Queuing Telemetry Transport (MQTT). It is a lightweight transmission or messaging protocol. Besides its little size, low control utilization, right off the bat, I will experience the motivation behind utilizing MQTT, how it works for all intents and purposes works with a genuine IoT model. At that point, I will experience the broker; the foundation of the MQTT. Why we have used MQTT is because of the steps mentioned below about MQTT.

MQTT has one of the kindest highlights you can scarcely discover in different protocols, as:

- A protocol with light weight. Thus, it's anything but difficult to actualize in software and quick in the transmission of information.
- It depends on the information type and method of the message. Obviously, we know how quickly the information flows.
- Limited information packets. Thus, low organize utilization.
- Utilization of power is very low.
- Works on real-time data which makes it a perfect match of the devices of IOT.

How MQTT works

MQTT server is known as a broker and the customers are just the associated gadgets. At the point when a customer wants to send information to the broker, we consider this activity as a "Publisher". At the point when a customer wants to get information from the broker, we consider this activity as a "subscribe".

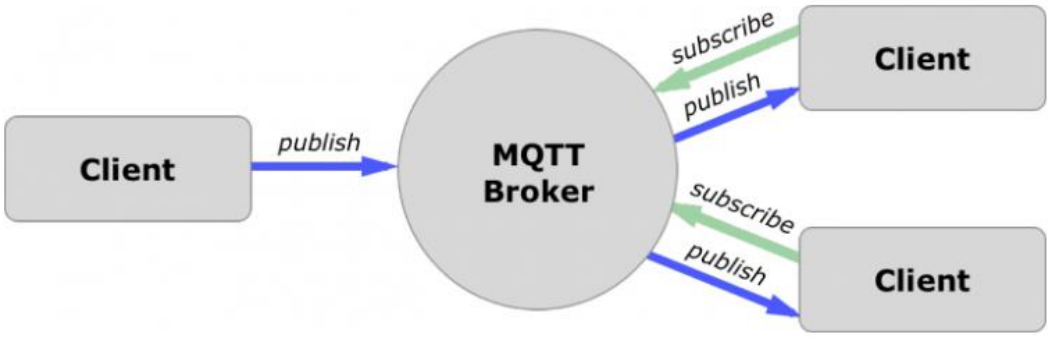

Figure 16:*MQTT working model [ ]*

4.3.4 Control System

The third step is to control the flow of our framework. For this purpose, we have used different checks to control the information or message flow. This message flow also controls the liveness aspect that if the message is not delivered or lost at any stage it will request liveness to resend it. In our case the information is water flow, meaning if the water level decreases from the certain level, it will generate an alarm.

4.3.5 Security

Security is the most important aspect in any field. For this, we have secure ports and have applied different checks and avoid malicious script to overcome the security threats. Liveness is also a part of authentication, and for security as well.

4.3.6 Targeted CPS

The final step of our suggested framework is targeted Cyber-physical System or a receiver. This targeted CPS may be located outside the city. We have shown in our simulation that two CPSs are located in two different cities and information is passed through WAN using MQTT protocol. This is the place where the information or message is arriving or received. Where the source message or information is destined to go and where it is confirmed that the desired information or message arrived successfully which is triggered from the source without any loss of information. Hence, the received information is correct.

Chapter 5

Evaluation and Findings

Overview

This chapter briefly explains the validation of our implemented framework for CPSs. In this thesis, we have introduced a new technique for safety and security framework for CPSs using MQTT protocol.

5.1 Results and discussion

This section describes the overall flow and working of the proposed system using MQTT framework. We have also applied DDOS attack to check our security framework, but the results shown the immunity of our framework for CPSs.

The below mentioned figures (17 & 18) are about the starting and stopping of the button for the flow of information.

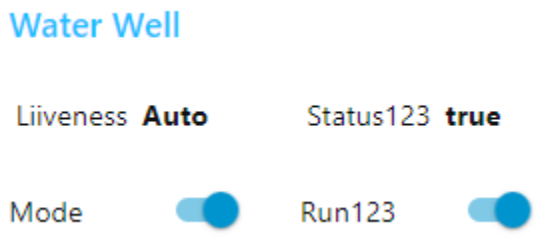

Figure 17: *Starting the Water flow*

```
[info] [function:Remote] Sensors false
[info] [function:Remote] Sensors true
```

Figure 18*:Output of Starting the Water flow*

The above two figures clearly show when the start (run) hits we can see the status in our mosquito's broker sensors and the information flows accordingly. Graphical output is shown in the image given below in the form of charts.

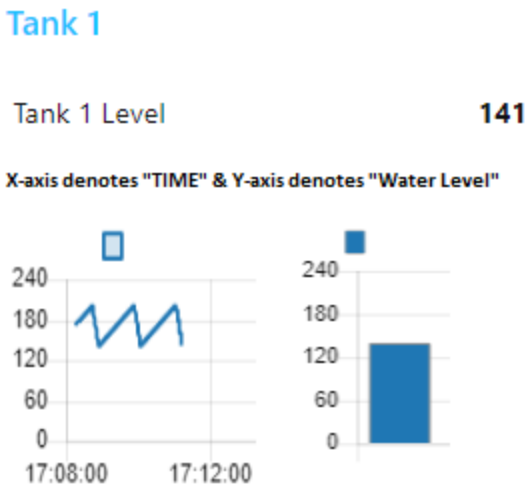

***Figure 19**:Graphical output after starting the run button*

The below figures depicts the run button's state

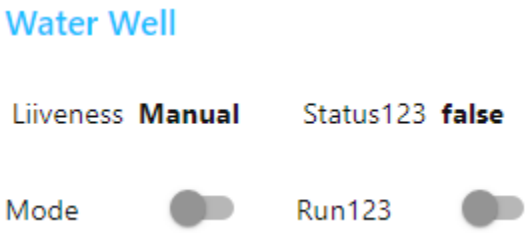

***Figure 20:**Graphical output after starting the run button*

```
[info] [function:Remote] Sensors false
[info] [function:Remote] Sensors true
```

***Figure 21:**Output of stopping the Water flow in mosquito broker*

5.1.1 LOIC

LOIC is an attacking instrument in the world of cyber.This attacking application created by 4Chan-partnered. This instrument puts the capacity to dispatch DDoS and DOS attacks in the hands of clients with almost no specialized learning.

5.1.2 Attacking and results

We have used LOIC (Low Orbit Ion Canon) to apply an attack on our security framework. The below figures show that the attack was applied in our security framework, but the information flow is normal.

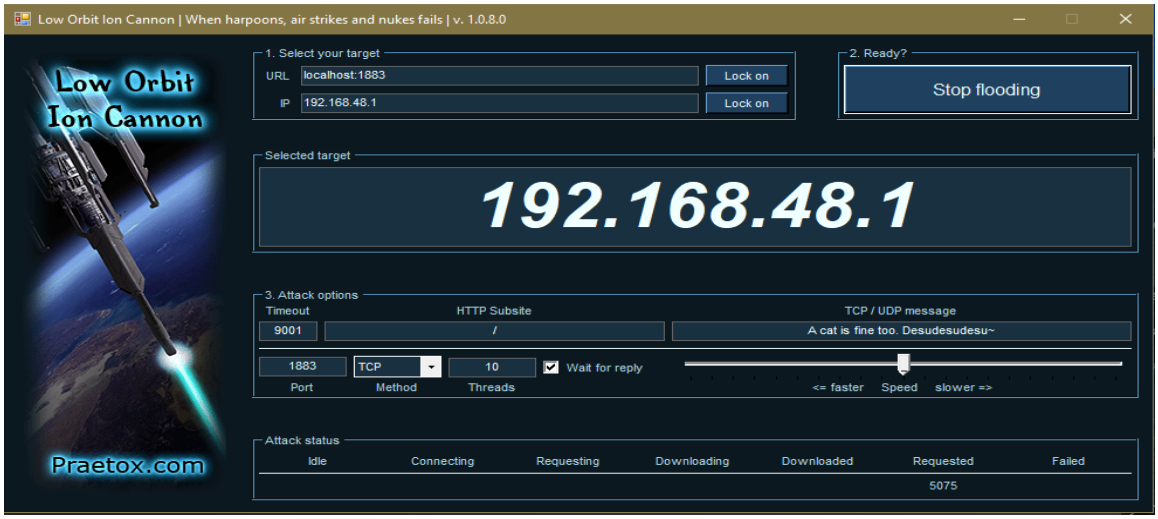

Figure 22:*LOIC DDOS attack on Proposed Framework*

192.168.48.1 is the IP of our system which is used by the Node-red on port 1880 and MQTT is running with the same IP but on port 1883.

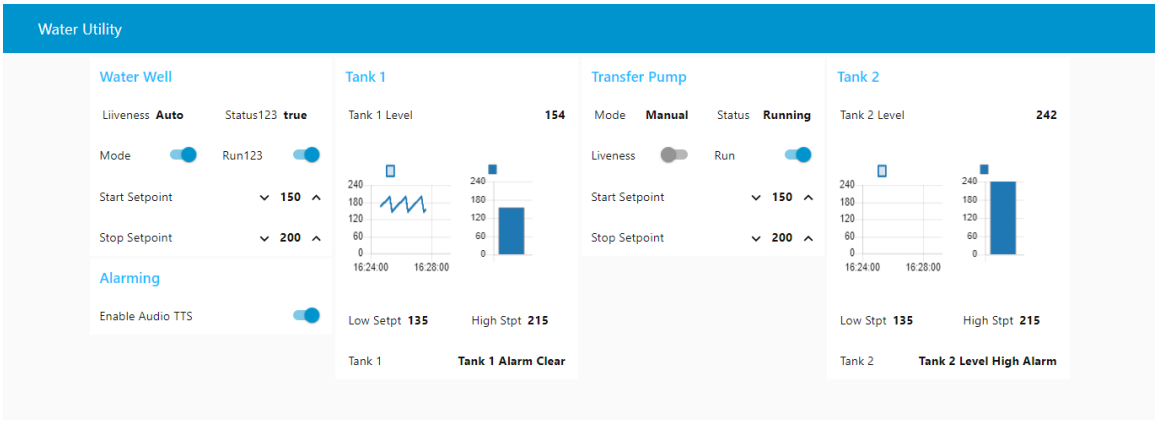

***Figure 23**:While LOIC throwing DDOS attack on our Proposed Framework*

The above figure shows the immunity of our applied framework. Where the value of the start point is greater than or equal to 150 and the stop point is 200.Alarm alert is working fine in the form of audio on the other hand. In chapter 2 section 2.3 (Figure 10,11&12), we have implemented the framework defined in reference #4 and applied DDOS to check the immunity of their framework but the system got stuck. In this study, we have proved the importance of liveness by implementing and comparing our proposed framework with the other.

Chapter 6

Conclusion

In this research, we have developed a framework for safety and security of CPS using MQTT (Message Queue Telemetery Transport) Protocol. Although, different techniques are used to build a framework for the safety and security of CPS, however, we have introduced our own framework that utilizes the MQTT protocol. With the help of our framework we have tried to secure the CPSs. We have used NODE-RED (a simulation tool) to build this framework. We have developed a water SCADA system which transfers the water from source CPS to the targeted CPS, which is located in different places. Further, we have secured the communication between these two CPSs with the help of Liveness. We have also implemented DDOS (Distributed Denial Of Service) attack on our implemented framework to check the immunity of our proposed security framework. Moreover, we have shown the normality or immunity of our safety and security framework for CPSs. We have also implemented the framework of "Utku Ozgur" and applied DDOS attack to check the immunity, but the system got stuck. Hence, more research and development work is required for the safety and security of CPSs in the light of artificial Intelligence.

References

[1]. Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-Physical Systems Security—A Survey. IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 6, DECEMBER 2017

[2] Rehman, S.U.; Gruhn, V. An Effective Security Requirements Engineering Framework for Cyber-Physical Systems. Technologies2018, 6, 65.

[3] P. Dong, Y. Han, X. Guo, F. Xie, "A Security and safety Framework for Cyber Physical System", International Conference on Control and Automation, 2014.

[4] Utku Ozgur ; Harikrishnan T. Nair ; Aditya Sundararajan ; Kemal Akkaya ; Arif I. Sarwat An efficient MQTT framework for control and protection of networked cyber-physical systems. 9-11 Oct. 2017 . 2017 IEEE Conference on Communications and Network Security (CNS)

[5] DiMase, D., Collier, Z.A., Heffner, K. et al. Environ Syst Decis (2015) 35: 291. https://doi.org/10.1007/s10669-015-9540-y

[6] Adam Hahn, Roshan K.Thomas ,Ivan Lozano, Alvaro Cardenas.” A multi-layered and kill-chain based security analysis framework for cyber-physical systems”. https://doi.org/10.1016/j.ijcip.2015.08.003

[7] Lu, T., Zhao, J., Zhao, L., Li, Y., and Zhang, X., “Towards a Framework for Assuring Cyber Physical System Security,” International Journal of Security&Its Applications, Vol. 9, No. 3, pp. 25–40, 2015.

[8]A. Khalid, P. Kirisci, Z.H. Khan, Z. Ghrairi, K.-D. Thoben, J. Pannek.” Security framework for industrial collaborative robotic cyber-physical systems “Comput. Ind., 97 (2018), pp. 123-145, 10.1016/j.compind.2018.02.009.

[9] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, “A survey on security control and attack detection for industrial cyber-physical systems,” Neurocomputing, to be published, doi: 10.1016/j.neucom.2017.10.009

[10] P. Leita˜o, J. Barbosa, M.-E. C. Papadopoulou, and I. S. Venieris, “Standardization in cyber-physical systems: The ARUM case,” in Proc. IEEE Int. Conf. Ind. Technol., Mar. 2015, pp. 2988–2993.

[11] K. Paridari, A. E.-D. Mady, S. La Porta, R. Chabukswar, J. Blanco, A. Teixeira, H. Sandberg, and M. Boubekeur, “Cyber-physical-security framework for building energy management system,” in 7th International Conference of Cyber-Physical Systems (ICCPS), 2016

[12] S. F. Ochoa, G. Fortino, and G. Di Fatta, ‘‘Cyber-physical systems, Internet of Things and big data,’’ Future Generat. Comput. Syst., vol 75, pp. 82–84, Oct. 2017.

[13] S. R. Chhetri, J. Wan, and M. A. Al Faruque, “Cross-domain security of cyber-physical systems,” in Design Automation Conference (ASP-DAC), 2017 22nd Asia and South Pacific, pp. 200–205, IEEE, 2017.

[14] He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., Gabrys, B., 2016. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In: 2016 IEEE Congress on Evolutionary Computation, CEC 2016 7743900. pp. 1015–1021.

[15] Tianbo Lu, Jiaxi Lin, Lingling Zhao, Yang Li, and Yong Peng. 2015. A Security Architecture in Cyber-Physical Systems: Security Theories, Analysis, Simulation and Application Fields. International Journal of Security and Its Applications 9, 7 (2015), 1–16.

[16] Christoph Schmittner, Zhendong Ma, Erwin Schoitsch, and Thomas Gruber. A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, pages 69–80. ACM, 2015.

[17] A. Chattopadhyay, A. Prakash, M. Shafique, Secure cyber-physical systems: Current trends, tools and open research problems, in: Design, 27 Automation Test in Europe Conference Exhibition (DATE), 2017, pp. 1104–1109.

[18] I. Dumitrache, I.S. Sacala, M.A. Moisescu, S.I. Caramina, “A conceptual framework for modeling and design of Cyber-Physical Systems”, Studies in Informatics and Control, Vol. 26, No. 3, pp. 325-334, 2017.

[19] Y. Zacchia Lun, A. D’Innocenzo, I. Malavolta, and M. D. Di Benedetto. Cyber-Physical Systems Security: a Systematic Mapping Study. CoRR, abs/1605.09641, 2016.

[20] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, “A survey on smart grid cyber-physical system testbeds,” IEEE Communications Surveys http://ieeexplore.ieee.org/abstract/document/7740849/

[21] Y. Wang, Z. Lin, X. Liang, W. Xu, Q. Yang, and G. Yan, ‘‘On modeling of electrical cyber-physical systems considering cyber security,’’ Frontiers Inf. Technol. Electron. Eng., vol. 17, no. 5, pp. 465–478, 2016.

[22] X. Yu and Y. Xue, “Smart grids: A cyber–physical systems perspective,” Proceedings of the IEEE, vol. 104, no. 5, pp. 1058–1070, may 2016.

[23] Tianbo Lu, Jinyang Zhao, Lingling Zhao, Yang Li, and Xiaoyan Zhang, "Towards a Framework for Assuring Cyber Physical System Security," International Journal of Security and its Applications, vol. 9, no. 3, pp. 25-40, 2015.

[24] A. Sanjab and W. Saad, “On Bounded Rationality in Cyber-Physical Systems Security: Game-Theoretic Analysis with Application to Smart Grid Protection,” 2016. [Online]. Available: http://arxiv.org/abs/1610.02110

[25] O. Younis and N. Moayeri, “Cyber-physical systems: A framework for dynamic traffic light control at road intersections,” 2016 IEEE Wirel. Commun. Netw. Conf., vol. 4, no. 6, pp. 1–6, 2016.

[26] V.K. Sehgal, A. Patrick, A. Soni, and L. Rajput, “Smart Human Security Framework Using Internet of Things, Cloud and Fog Computing,” in Proc. of Intelligent Distributed Computing, 2015, pp. 251–263.

[27] https://flows.nodered.org/flow/b1d00d13f1db357ac686f9379731060c

[28] https://1sheeld.com/mqtt-protocol/

[29] G. Sabaliauskaite and A. P. Mathur, “Aligning Cyber-Physical System Safety and Security,” in 1st Asia - Pacific Conf. on Complex Systems Design & Management, CSD&M, 2014, pp. 41–53.

[30] V. De Florio and G. Primiero, “A framework for trustworthiness assessment based on fidelity in cyber and physical domains,” The 6th International Conference on Ambient Systems, Networks and Technologies, vol. 52, pp. 996–1003, 2015.

[31] W. Grega, A.J. Kornechi, "Real-Time Cyber-Physical Systems - Transatlantic Engineering Curricula Framework", Proc. of Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 767-774, 2015.

[32] K.-K. R. Choo, M. M. Kermani, R. Azarderakhsh, M. Govindarasu, "Emerging embedded and cyber physical system security challenges and innovations", IEEE Trans. Dependable Secure Comput., vol. 14, no. 3, pp. 235-236, May/Jun. 2017

[33] Oks, S. J., Fritzsche, A., and Möslein, K. M. 2017. “An Application Map for Industrial CyberPhysical Systems.” In: Industrial Internet of Things. Springer International Publishing: 21-46.

[34] Goh, J.; Adepu, S.; Tan, M.; Lee, Z.S. Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks. In Proceedings of the 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 12–14 January 2017; pp. 140–145.

[35] Lun, Y.Z.; D’Innocenzo, A.; Smarra, F.; Malavolta, I.; Di Benedetto, M.D. State of the art of cyber-physical systems security: An automatic control perspective. J. Syst. Softw. 2019, 149, 174–216.

[36] C. Alcaraz, J. Lopez, Secure interoperability in cyber-physical systems, in: Security Solutions and Applied Cryptography in Smart Grid Communications, IGI Global, USA, IGI Global, USA, 2017, Ch. 8, pp. 137–158.

[37] McKee, D.W. Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems. CAAI Trans. Intell. Technol. 2018, 3, 75–82.

[39] A. Ferdowsi, W. Saad, B. Maham, and N. B. Mandayam, “A Colonel Blotto game for interdependence-aware cyber-physical systems security in smart cities,” in Proceedings of the 2nd International Workshop on Science of Smart City Operations and Platforms Engineering, ser. SCOPE ’17. Pittsburgh, Pennsylvania: ACM, 2017, pp. 7–12

[40] B. Bordel, R. Alcarria, D. Sánchez-de-Rivera, and T. Robles, ‘‘Protecting industry 4.0 systems against the malicious effects of cyber-physical attacks,’’ in Proc. Int. Conf. Ubiquitous Comput. Ambient Intell. Cham, Switzerland: Springer, Nov. 2017, pp. 161–171.

[41] Ananth A. Jillepalli et al. “Security Management of Cyber Physical Control Systems Using NIST SP 800-82r2”, 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, 2017, pp. 1864-1870

[42] RASHID, A., DANEZIS, G., CHIVERS, H., LUPU, E., MARTIN, A., LEWIS, M., AND PEERSMAN, C. Scoping the Cyber Security Body of Knowledge. IEEE Security & Privacy (2018).

[43] Y. Wang, M. Amin, J. Fu, and H. Moussa, “A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids,” IEEE Access, 2017.