Vulnerabilities and Security Issues in Cps and IOT for Wire Less Communication

S.P. Maniraj, R. Pranay Sharma, M. Venkata Siva Kumar, B.V. Sai Mohan Krishna, G. Sree Ram Pavan

Abstract--- The concept of IoT stems from connected smart devices, which may or may not be connected physically via wires. The Cyber-Physical Systems, on the other hand are complex distributed systems, consisting of a large number of sensors and actuators, which are connected to a pool of computing nodes. With the fusion of sensors, computing nodes, and actuators, which are connected through various means of communications, CPSs aim to perceive and understand changes in the physical environment, analyse the impacts of such changes to their operation, and make intelligent decisions to respond to the changes. Thus, in both CPS and IoT wireless communication plays a very important role. With in increasing number of devices, the security against the manipulation of the sensor data is needed as a change in the input can change the behaviour of the system altogether. In this paper, we take a deeper look into the security issues and vulnerabilities of the wireless communication in both the Cyber Physical Systems (CPS) and the Internet of Things (IoT).

Keywords--- Distributed systems; nodes; manipulation; vulnerabilities.

I. INTRODUCTION

Cyber Physical System (CPS) [1] goes for checking the conduct of physical procedures, and impelling activities to change its conduct so as to make the physical condition work accurately and better. Ordinarily, a cyber physical system (CPS) comprises of two noteworthy segments, a physical procedure and a cyber framework. Commonly, the physical process is checked or constrained by the cyber framework, which is an organized arrangement of a few minor gadgets with detecting, processing and communication capabilities. However, as the communication between the physical and digital frameworks expands, the physical frameworks move toward becoming progressively increasingly helpless to the security vulnerabilities in the cyber framework.

In reality, the security vulnerabilities are being found in increasingly more cyber physical frameworks like electronic power framework, smart transportation frameworks, medicinal frameworks, and so on. It is required to develop a network which connects many number of systems into a single unit wireless sensor networking is the vital technology for ubiquitous system. This resulted in the concern of the analysts and researchers as they were worried about the security of CPS. When the advancement in technology is high and when there are more confidential and exceedingly smarter cyber physical frameworks, there should be a cautious thought about the conceivable vulnerabilities on these systems. As a matter of fact, vulnerabilities for cyber physical frameworks is a moderately new area and very little work has been done in this domain. Like some other new fields, most of the efforts are to concentrated on mapping arrangements from existing spaces, for example, sensor systems which share the organized activity and low capacity attributes with CPS.

II. LITERATURE SURVEY

Security Issues and Challenges for Cyber Physical System.

Authors- Eric Ke Wang, Yunming Ye, Xiaofei Xu This paper examines the security challenges also, issues of cyber physical frameworks. The abstract of the general work process of cyber physical frameworks, the identification of the conceivable vulnerabilities, assault issues, enemies attributes and a lot of difficulties that should be tended to and the additional propose on a contextual security structure for general cyber physical frameworks and some potential research regions and issues are proposed.

Security Challenges for Medical Devices

Authors- J Sametinger, J Rozenblit, R Lysecky & P Otto In this paper the major agenda of the project relies on the providing the security to the Medical Devices. There are many devices which had been invented in the medicine stream. Any type of improper care towards these devices may definitely ruin the life of the patients. It includes both the hardware and software components that are used in building these devices. There are many organizations to regulate the proper work of the manufacturing devices like FDA(Food and Drugs Administration) and WHO(World Health Organization).

Zigbee Technology in future data communication system.

Authors- Sushila Gupta

Due to dramatic change in pervasive computation where desktop model is replaced with ubiquitous computing ideal, this leads to necessity of developing the standard protocol to solve the challenges, they are even complex compared to a peripheral connecting to a p.c. Zig-bee, an emerging standard within networked embedded systems. Zigbee solves the issues like reliability, global usage, remotely up gradable firmware, low-power & maintenance.

Revised Version Manuscript Received on 22 February, 2019

S.P. Maniraj, Asst.Professor, SRM Institute of Science and Technology, Chennai. (e-mail: spmaniraj@gmail.com)

R. Pranay Sharma, UG Scholar, SRM Institute of Science and Technology, Chennai. (e-mail: rps2579@gmail.com)

M. Venkata Siva Kumar, UG Scholar, SRM Institute of Science and Technology, Chennai. (e-mail: malinenivenkat22@gmail.com)

B.V. Sai Mohan Krishna, UG Scholar, SRM Institute of Science and Technology, Chennai. (e-mail: bvsaimohankrishna@gmail.com)

G. Sree Ram Pavan, UG Scholar, SRM Institute of Science and Technology, Chennai. (e-mail: gsrpavan29@gmail.com)

Optimal Attack Strategies Subject to Detection Constraints against Cyber-Physical Systems

Authors-Yuan Chen, Soummya Kar, and Jos´e M. F. Moura

Because of sensational change in inescapable calculation where work area show is supplanted with universal processing perfect, this prompts need of building up the standard convention to fathom the difficulties; they are even perplexing contrasted with a fringe associating with a p.c. Zigbee, a rising standard inside arranged installed systems. Zigbee illuminates the issues like dependability, worldwide use, remotely up gradable firmware, low-control and upkeep.

A survey on CPS Maintenance

Authors- J. Shi,J. Wan, H. Yan, and H. Suo This paper mainly concentrates on the Intelligent Maintenance Systems (IMS). IMS are data acquirement examination structures for insightful help. The IMS give self-administer conclusions, prognostics, and prosperity evaluation of sections. Here, this examination has used a CPS approach to manage consider the alternate points of view present into an upkeep area. The CPS is another perspective that attempts to combine and mastermind physical and computational segments. In this paper, they propose a 2D/3D portrayal mechanical assembly for computerized physical upkeep circumstances. This instrument works under HTTP tradition and makes it possible for the progressing portrayal and remotely getting to empowering customers to see, to adjust and to get to the help data by web program.

III. PROPOSED SYSTEM

As there are lot of problems emerging in the security field of the Cyber physical systems, this paper provides various methods for various problems which have been existed in the literature survey to rectify the problem using various algorithms and techniques which will thus help to rectify the issue.

Issues in Existing Systems

Issue1

In [43], there is problem mentioned which majorly deals with the issues in the Bluetooth technology, when a comparative study is made with the Zigbee technology. The solution, rather a proposal on how the problem can be dealt is given below as another technology, which is by Near Field Communication.

NFC is a creating remote short-run correspondence development that relies upon existing standards of the Radio Frequency Identification (RFID) establishment. The objective of this paper is to portray key characteristics and benefits of the basic advancement, to mastermind techniques for action and to display distinctive use cases. Additionally, security concerns, challenges, and present clashes talked about in it.

How it can be helpful?

The cell phone advertise anyway is as of now developing immensely. When entering the show room, the authenticity of the ticket can be embraced by simply waving the phone over a NFC per client contraption at the entry control. In the wake of having had a great time the execution, the visitor could share photos he's taken in the midst of the show with another visitor by basically holding their two phones together.

Likewise, just to seek after this circumstance when taking the vehicle home a brief span later, the customer isn't required to dully aggregate coins the get a vehicle ticket at the dealer machine. Or maybe, when entering and leaving the vehicle, he contacts his phone to a for every client contraption and the most economical ticket cost is normally charged from his record. This showed circumstance wonderfully focuses possible key benefit of inevitable correspondence overseen by NFC advancement: a greater dimension of flexibility and straightforwardness while decreasing the proportion of physical effort required.

Problems of using NFC

At present, the NFC advancement has accomplished a measurement where business dispatch arranging can begin and should be developed. Regardless, somewhat definite measures for NFC organizations are missing. The nonattendance of an outrageous unquestionable philosophy for the headway of NFC organizations begins in a fundamental conflict between a couple of included key performing craftsmen including PDA makes, sort out overseers, banks, and other master associations: each social occasion beyond question attempts to approve its interests and needs to accept an imperative employment in the line of the application circumstance, and the accomplice getting of tremendous money.

Issue2

In survey paper C, there is problem mentioned which majorly deals with the issues in ubiquitous system. As a result of this ubiquitous system, a high level communication protocols is required to generate with small, low-power digital radios, which can be utilized for automation of home appliances and collection of medical device data. Availability is the key issue in the future for wireless sensor networking. To overcome this issue, this paper proposes the idea of using Zigbee Technology to this system which is further explained below.

How it can be helpful?

Zig-bee/IEEE 802.15.4 is available with data transmission rates varying from 20 to 900 kilobits/second. Zig-bee can define if there is any periodicity or repetition in the data or if the data is intermittent. Zig-bee employs two types of modes:

- **Beacon mode**: It is used when the coordinator runs on batteries so that maximum power savings is achieved in this mode. In this device, coordinators observe the beacon which gets transmitted periodically. Post transmission, the coordinator sets a schedule for the next beacon so that device “goes to sleep”. In other way coordinator itself switches to sleep mode. The devices in mesh network know when to communicate with each other.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- **Non Beacon Mode:** It will come out of the sleep mode and the continued availability in the network at random intervals is confirmed.

Issue3

In survey paper C, there is problem mentioned which majorly deals with the issues in the CPS inputs that are mainly provided by the sensors through wireless communication. The wireless communication works based on frequency of sender and receiver and any receptor within the region that can catch the frequency of the sensor can manipulate the input and send a garbage value / other value with the same frequency as that from the sensor. This results in the processing of the wrong inputs which may lead to unwanted behaviour from the CPS. This can affect the system on many levels which can lead to shut down of the systems too.

How it can be helpful?

This paper provides an additional level of security by adding to the intelligence of the system. We propose an *input pre-processing layer* after the reception of input from sensors. During the development stages and the initial usage days of the CPS newly being setup for a purpose, we can gather a set of variable values and its general communication frequency of values (the time span in which the system usually communicates with the CPS by sending inputs). This can be analyzed to establish a sensor network behaviour pattern which is set in the CPS. Whenever an input is received, the system can first check the input with the pattern of input over the sensor's lifetime in the network. If the input is found abnormal, it can be compared with the other sensor input values from the nearby sensors. Also it can hold the input for some time to compare with the next value.

Another proposal is a hardware and software combination modification. On any irregular value reception from the sensor, the system shall communicate to a nearby sensor and send the signal to the *misbehaving sensor* through the nearby sensor to change its frequency and communicate the same value and a new value from the newly set frequency. In addition the sensor also communicates the new value again in the normal frequency of it. If multiple inputs are received now, then the sensor can be deemed as *infected by* hacker and its inputs can be neglected until the issue is resolved. This is another way in which a new layer can aid in better security and provide integrity, consistency to the values being communicated from the sensors.

An alternative approach for the better security of CPS devices

In parallel to the recent and ongoing extension of cellular networks to better support CPS and IoT communication, a new class of communication standards and networks has recently emerged. The two most prominent proprietary standards of this class are LoRa (cf., Fig. 10) and SigFox. The objective of both systems is to support a massive number of ultra-low-rate and ultra-low-power wireless sensors and devices.

These low-power wide area networks are similar to cellular networks, but operate in the unlicensed ISM bands, which simplifies and opens the deployment of the necessary infrastructure to anyone. The LPWAN structure resembles more a mesh network than a cellular network since signals can be picked up by multiple base stations (gateways), which improve reliability, especially in an unmanaged network. An important focus of the PHY layer of these systems is to achieve a high sensitivity to maximize the radio reach. This strategy guarantees a good coverage even in occluded areas and reduces the number of gateways and hence the cost of the required infrastructure.

IV. SYSTEM ARCHITECTURE

In the proposed system, there are 4 modules.

- Physical Module: This module deals with the sensors and actuators.
- Wireless Module: The communication between Sensors, actuators and centralized systems in the Cyber Space.
- Detection Module: The proposed module which analyses the flow of input into the centralised systems from the wireless module.
- Controller Module: The user interface and the control algorithms process the inputs and the changes are reverted to the UI, thus enabling the autonomous environment.

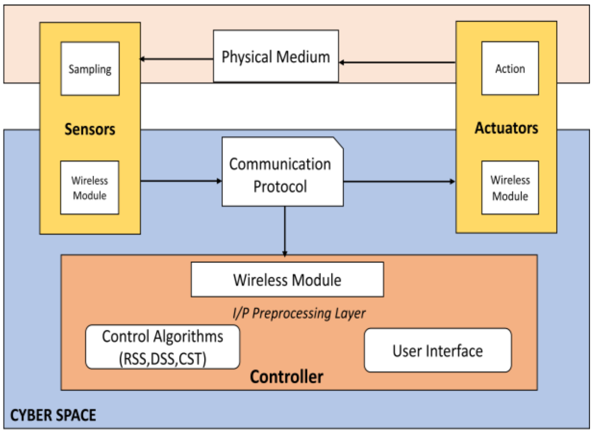

Fig 4.1 System Architecture

V. ADVANTAGES OF PROPOSED SYSTEM

- Advancement in Cyber Physical System.
- Providing high levels of security through encryption.
- Interconnectivity of both CPS and IOT.
- Better interoperability of devices.

VI. CONCLUSION AND FUTURE WORKS

Classical security measures are applied at the MAC/ DLL, network, transport, and application layer and corresponding techniques are based on standard cryptographic principles. While a variety of MAC layer protocols exist, we only consider three general strategies. We also limit our discussion to time-division duplexing (TDD) rather than frequency-division duplexing (FDD) for multiplexing the uplink and downlink communication between a node and a central access point or another node.

TDD is more common than FDD in most low-power wireless systems since it allows for a more flexible resource allocation between the two directions and avoids the cost/power overhead for concurrently operating on two different carrier frequencies.

REFERENCES

1. J. Shi, J. Wan, H. Yan, and H. Suo, “A survey of cyber-physical systems,” in *Proc. Int. Conf. Wireless Commun. Signal Process.*, Nov. 2011, pp. 1–6, doi: 10.1109/WCSP.2011.6096958.
2. A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber physical systems security—A survey,” *CoRR*,2017.
3. A. Chattopadhyay, A. Prakash, and M. Shafique, “Secure cyber-physical systems: Current trends, tools and open research problems,” in *Proc. DATE*, 2017, pp. 1104–1109.
4. R. Want, “Near field communication,” I*EEE Pervasive Comput.*, vol. 10, no. 3, pp. 4–7,Mar. 2011.
5. A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, “Towards threat of implementation attacks on substation security: Case study on fault detection and isolation,” *IEEE Trans. Ind. Informat.*,2017, doi: 10.1109/TII.2017.2770096.
6. A. Wheeler, “Commercial applications of wireless sensor networks using ZigBee,” *IEEE Commun. Mag.*, vol. 45, no. 4, pp. 70–77, Apr. 2007, doi: 10.1109/MCOM.2007.343615.
7. Y. Mo and B. Sinopoli, “Integrity attacks on cyber-physical systems,” in Proc. of the 1st ACM International Conf. on High Confidence Networked Systems, Beijing, China, Apr. 2012, pp. 47–54.
8. Y. Zou, J. Zhu, X. Wang, and L. Hanzo,“A survey on wireless security: technical challenges, recent advances, and future trends,” *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/ JPROC.2016.2558521.
9. I. Butun, S. D. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014, doi: 10.1109/ SURV.2013.050113.00191.
10. J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, “Security challenges for medical devices,” *Commun. ACM*, vol. 58, pp. 74–82, Mar. 2015, doi: 10.1145/2667218.
11. B. Zhu, A. Joseph, and S. Sastry, “A taxonomy of cyber attacks on SCADA systems,” in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber Phys. Soc. Comput.*, Oct. 2011, pp. 380–388, doi: 10.1109/ iThings/CPSCom.2011.34.
12. C. Gomez and J. Paradells, “Wireless home automation networks: A survey of architectures and technologies,” *IEEE Commun. Mag.*, vol. 48, no. 6, pp. 92–101, Jun. 2010, doi: 10.1109/ MCOM.2010.5473869.
13. S. S. R. Ahamed, “The role of ZigBee technology in future data communication system,” *J. Theor. Appl. Inf. Technol.*, vol. 5, no. 2, p. 29, 2009.
14. M. Zhou and Z.-L. Nie, “Analysis and design of ZigBee MAC layers protocol,” in *Proc. Int. Conf. Future Inf. Technol. Manage. Eng.*, vol. 2. Oct. 2010, pp. 211– 15, doi: 10.1109/ FITME.2010.5654824.
15. Y. Mo and B. Sinopoli, “False data injection attacks in control systems,” In Proc. of the 1st Workshop on Secure Control Systems, Stockholm, Sweden, Apr. 2010, pp. 56–62.