IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 120-125
www.iosrjournals.org

Analysis of Intrusion Detection Response System (IDRS) In Cyber Physical Systems (Cps) Using Regular Expression (Regexp)

Ms. Simrandeep Kaur chana*, Prof S.J.Karale**
**(Department of Computer Science & Engineering, Nagpur University, Nagpur*
*** (Department of Information Technology, Nagpur University, Nagpur*

***Abstract**: In this research we aim to design and validate Intrusion Detection Response System (IDRS) for a cyber physical system (CPS) comprising for controlling and protecting physical infrastructures. The design part includes host IDS, system IDS and IDS response designs. The validation part includes a novel model-based analysis methodology with simulation validation. Our objective is to maximize the CPS reliability or lifetime in the presence of malicious nodes performing attacks which can cause security failures. Our host IDS design results in a lightweight, accurate, autonomous and adaptive protocol that runs on every node in the CPS to detect misbehavior of neighbor nodes based on state-based behavior specifications. Our system IDS design results in a robust and resilient protocol that can cope with malicious, erroneous, partly trusted, uncertain and incomplete information in a CPS. Our IDS response design results in a highly adaptive and dynamic control protocol that can adjust detection strength in response to environment changes in attacker strength and behavior. The end result is an energy-aware and adaptive IDS that can maximize the CPS lifetime in the presence of malicious attacks, as well as malicious, erroneous, partly trusted, uncertain and incomplete information.*

We develop a probability model based on regular expression technique to describe the behavior of a CPS incorporating our proposed intrusion detection and response designs, subject to attacks by malicious nodes exhibiting a range of attacker behaviors, including reckless, random, insidious and opportunistic attacker models. We identify optimal intrusion detection settings under which the CPS reliability or lifetime is maximized for each attacker model. Adaptive control for maximizing IDS performance is achieved by dynamically adjusting detection and response strength in response to attacker strength and behavior detected at runtime.
***Keywords:** Cyber Physical system, Intrusion Detection, Intrusion Response, Regular Expressions.*

I. Introduction

Recent years have seen a dramatic rise in the development of smart and context-aware systems that present a tight coupling between embedded computing devices and their physical environment. Representative examples include: 1) physiological sensors deployed on human body that continuously monitor the health and enable fast detection of medical emergencies and the delivery of therapies; 2) smart buildings that detects absence of occupants and shut down the cooling unit to save energy; 3) data centers that use solar energy for cooling purposes; 4) unmanned aerial vehicles (UAVs) that use an image of the terrain to perform surveillance. A common theme in such smart systems is the role played by the underlying physical environment. The physical environment provides information necessary for achieving many of the important functionalities. Systems that use the information from the physical environment during their operation, are cyber-physical systems (CPSs). Cyber Physical Systems (CPSs) are integrations of computation with physical processes. Cyber-physical systems (CPSs) have been at the core of critical infrastructures and industrial control systems for many decades, and yet, there have been few confirmed cases of computer-based attacks. CPS, however, are becoming more vulnerable to computer attacks for many reasons [1]. Cybercriminals compromise computers anywhere they can find them (even in control systems). These attacks may not be targeted (i.e., they do not have the intention of harming control systems), but may cause negative side effects: control systems infected with malware may operate inappropriately. Disgruntled employees are currently the major source of targeted computer attacks against control systems. These attacks are important from a security point of view because they are caused by insiders: individuals with authorized access to computers and networks used by control systems; so even if control networks were completely isolated from public networks (and the Internet), attacks by insiders would still be possible [5].

This research mainly aims to write a system that is used to analyze the effect of intrusion detection and response on the reliability of a cyber physical system (CPS) and protecting a physical infrastructure. We develop a probability model based on stochastic Petri nets that use Regular Expressions to describe the behavior of the CPS in the presence of both malicious nodes exhibiting a range of attacker behave, and an intrusion detection and response system (IDRS) for detecting and responding to malicious events at runtime.

The benefit of the system is that we will be able to identify the best detection strength (in terms of the detection interval and the number of detectors), and the best response strength (in terms of the per-host minimum compliance threshold for setting the false positive and negative probabilities), under which the reliability of the system may be maximized.

II. Objectives

The Proposed System tends to achieve the following objectives:-

2.1 Reliability

This system addresses the reliability issue of a CPS designed to sustain malicious attacks over a prolonged mission period without energy replenishment.

2.2 Best Detection Strength

This system will allow us to identify the best detection strength in terms of the detection interval and the number of detectors.

2.3 Best Response Strength

This system will provide the best response strength in terms of the per-host minimum compliance threshold for setting the false positive and negative probabilities.

III. Literature Review

Cyber Physical Systems are large scale, geographically dispersed, federated, hetero generous, life-critical systems that comprise sensors, actuators and control and networking components [4]. Cyber Physical Systems (CPSs) are large scale, geographically dispersed, federated, heterogeneous, life-critical systems therefore securing CPSs has emerged as a critical interest of all governments[2]. The literature also refers to a CPS as a Distributed Control System (DCS), Networked Control System (NCS), Sensor Actuator Network (SAN), Supervisory Control and Data Acquisition (SCADA) system or Wireless Industrial Sensor Network (WISN) [4]. Their functions in common are sensing (acquisition) and actuation (control). These systems have wireless segments and are heterogeneous and geographically dispersed. These systems may be federated, mobile, attended or completely inaccessible. *Enclaves* define the edges of the segments of the federated system. Nodes that contain the sensors and actuators are called Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs) or Programmable Logic Controllers (PLCs). RTUs may implement some limited tactical control functions. Data Acquisition Systems (DASs) aggregate readings from RTUs and adapt (bridge or tunnel) the local RTU protocol with the long-haul protocol shared with the control center (such as TCP). Data processing servers effect the business logic of the CPS; these may be high performance computing clouds that process large datasets produced by economical nodes. Historian servers collect, store and distribute data from sensors. Nodes that contain control logic and provide management services to a Human Machine Interface (HMI) are called Master Terminal Units (MTUs); in contrast with the RTUs, an MTU implements the broad strategic control functions [4].

CPSs share several properties: These systems use embedded computers and networks to monitor and control physical processes with feedback to integrate computation with the environment. They consist of a set of networked sensors, actuators, control processing units and communication devices. CPSs are application-specific (purpose-built). Some segments may be resource-constrained: A Wireless Sensor Network (WSN) or Wireless Sensor and Actor Network (WSAN) may form part of a CPS [5] [4].

Common CPS issues are: availability, reconfigurability, distributed control (distributed management), real-time operation (timeliness), fault-tolerance, scalability, autonomy, reliability, security, heterogeneity, federation and geographic dispersion . Timeliness is critical in CPSs because the environment can change quickly; control loops fail if their period is longer than expected. Automatic control techniques can address CPS reliability. However, security requires distinct measures from reliability. Moreover, compromised nodes may collude to deter or disrupt the CPS functionality. An effective yet energy efficient intrusion detection system (IDS) is of great interest to detect and evict compromised nodes from a CPS whose failure can cause dire consequences. NSF characterizes CPSs as time-critical, position ally precise, energy efficient systems deployed in hostile environments (due to hazardous materials or combatants, for example) that coordinate large scale activities (like war fighting),enhance human capabilities (with sensors or navigation, for example) and improve social welfare (via extended medical care or assisted living, for instance)[4].

A CPS often operates in a rough environment wherein energy replenishment is not possible, and nodes may be compromised (or captured) at times. Thus, an intrusion detection and response system (IDRS) must detect malicious nodes without unnecessarily wasting energy to prolong the system lifetime [2]. Intrusion detection system (IDS) design for CPSs has attracted considerable attention Detection techniques in general can be classified into three types: signature based, anomaly based, and specification based techniques. While the literature is abundant in the collection and analysis aspects of intrusion detection, the response aspect is little

treated. In particular, there is a gap with respect to intrusion detection and response. Our IDRS design addresses both intrusion detection and response issues, with the goal to maximize the CPS lifetime [1] [4].

This research for CPS reliability assessment is model based analysis. Specifically, we develop a probability model to assess the reliability property of a CPS equipped with an IDRS for detecting and responding to malicious events detected[1]. Untreated in the literature, we would consider a variety of attacker behaviors including persistent, random, and insidious attacker models, and identify the best design settings of the detection strength and response strength to best balance energy conservation versus intrusion tolerance for achieving high reliability, when given a set of parameter values characterizing the operational environment and network conditions. Parameterization of the model using the properties of the IDS system is one major contribution of the research [1].

IV. Proposed Work Plan

Module 1: Development of Cyber Physical System

We are developing a Cyber Physical System, based on a reference CPS which comprises of RTUs and MTU. The mobile nodes (RTUs) are capable of sensing physical environments as well as actuating and controlling the underlying physical objects in the CPS**.** MTU receives sensing data from the nodes and determines actions to be performed then.

Module 2: Development of Intrusion Module for the system

This module deals with designing a intrusion module for the system which can be used to detect the malicious attacks at the runtime. Here basically algorithm for designing intrusion detection system is chosen and implemented.

Module 3: Development of Intrusion Detection Module for the system

We are designing a multi-agent response system for intrusion detection using MASID algorithm i.e Multi-agent Secure Intrusion Detection Algorithm. In multi-agent system, multiple agents is being used, through the use of multiple agents intrusion detection process gets distributed. Thus this system may also be called as distributive and cooperative intrusion detection system.

Module 4: Checking the Response of the System for Reliability of CPSs

In the final phase we are trying to describe the behavior of the CPS in the presence of both malicious nodes exhibiting a range of attacker behaviors, and an intrusion detection and response system (IDRS) for detecting and responding to malicious events at runtime.

V. Researched Methodology

5.1 Reference CPS

Our reference CPS model is based on the CPS infrastructure described in comprising 128 sensor carrying mobile nodes. Each node uses its sensor to measure any detectable phenomena nearby, and ranges its neighbors periodically by transmitting a code division multiple access (CDMA) waveform. Neighbors receiving that waveform transform the timing of the code (1023 symbols) and carrier (915 MHz) into distance. Essentially, each node performs sensing and reporting functions to provide information to upper layer control devices to control and protect the CPS infrastructure, and in addition utilizes its ranging function for node localization and intrusion detection. The reference model is a special case of a single-enclave system with homogeneous nodes. The IDS functionality is distributed to all nodes in the system for intrusion and fault tolerance. On top of the sensor carrying mobile nodes sits an enclave control node responsible for setting system parameters in response to dynamically changing conditions such as changes of attacker strength. The control module is assumed to be fault and intrusion free through security and hardware protection mechanisms against capture attacks and hardware failure.

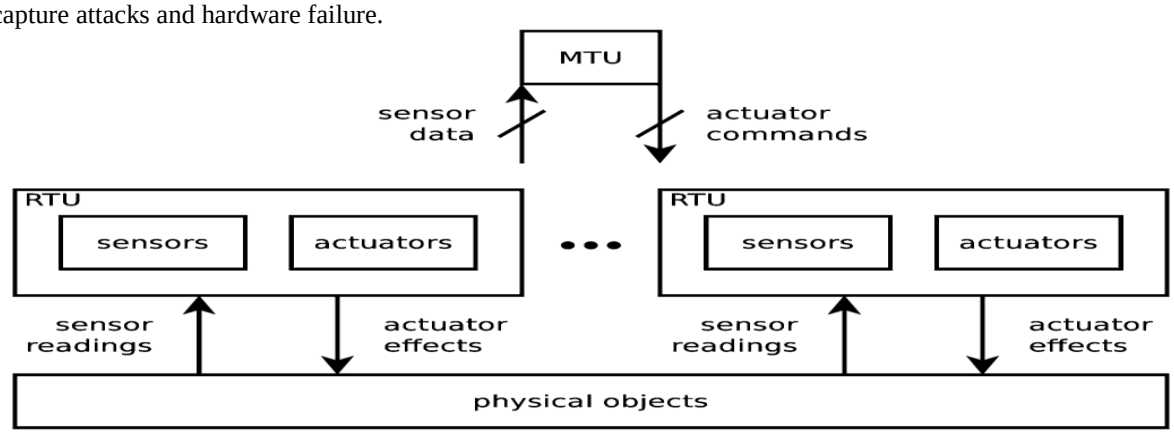

Figure1: Reference CPS

Fig. 1 contextualizes our reference CPS which comprises 128 sensor carrying mobile nodes, a control unit, and physical objects for controlling and protecting a physical infrastructure. The mobile nodes are capable of sensing physical environments, as well as actuating and controlling the underlying physical objects in the CPS. They function as sensors and actuators, each carrying sensors for sensing physical phenomena, as well as actuating devices for controlling physical objects. The CPS literature identifies these mobile nodes as remote terminal units (RTUs). Sitting on top of these mobile nodes is a control unit which receives sensing data from the mobile nodes and determines actions to be performed by individual nodes or a group of mobile nodes. The CPS literature identifies the control unit as the master terminal unit (MTU). The actions formulated by the MTU trigger actuating devices to control and protect the physical objects in the CPS.

5.2 Security Failure

We consider two security failure conditions. The first condition is based on the Byzantine fault model. That is, if one-third or more of the nodes are compromised, then the system fails. The reason is that once the system contains 1/3 or more compromised nodes, it is impossible to reach a consensus, hence inducing a security failure. The second condition is impairment failure. That is, a compromised CPS node performing active attacks without being detected can impair the functionality of the system and cause the system to fail. Impairment failure is modeled by defining an impairment-failure attack period by a compromised node beyond which the system cannot sustain the damage.

5.3 Attack Model

The first step in investigating network security is to define the attack model. We consider capture attacks which turn a good node into a bad insider node. We consider three attacker models: persistent, random, and insidious. A persistent attacker performs attacks with probability one (i.e., whenever it has a chance). The primary objective is to cause impairment failure. A random attacker performs attacks randomly with probability. The primary objective is to evade detection. An insidious attacker is hidden all the time to evade detection until a critical mass of compromised nodes is reached to perform "all in" attacks. The primary objective is to maximize the failure probability caused by either impairment or Byzantine security failure.

5.4 Host Intrusion Detection

Our host intrusion detection protocol design is based on two core techniques: behavior rule specification, and vector similarity specification. The basic idea of behavior rule specification is to specify the behavior of an entity (a sensor or an actuator) by a set of rules from which a state machine is automatically derived. Then, node misbehavior can be assessed by observing the behaviors of the node against the state machine (or behavior rules). The basic idea of vector similarity specification is to compare similarity of a sequence of sensor readings, commands, or votes among entities performing the same set of functions.

5.6 System Intrusion Detection

Our system IDS technique is based on majority voting of host IDS results to cope with incomplete and uncertain information available to nodes in the CPS. Our system-level IDS technique involves the selection of detectors as well as the invocation interval to best balance energy conservation versus intrusion tolerance for achieving high reliability.

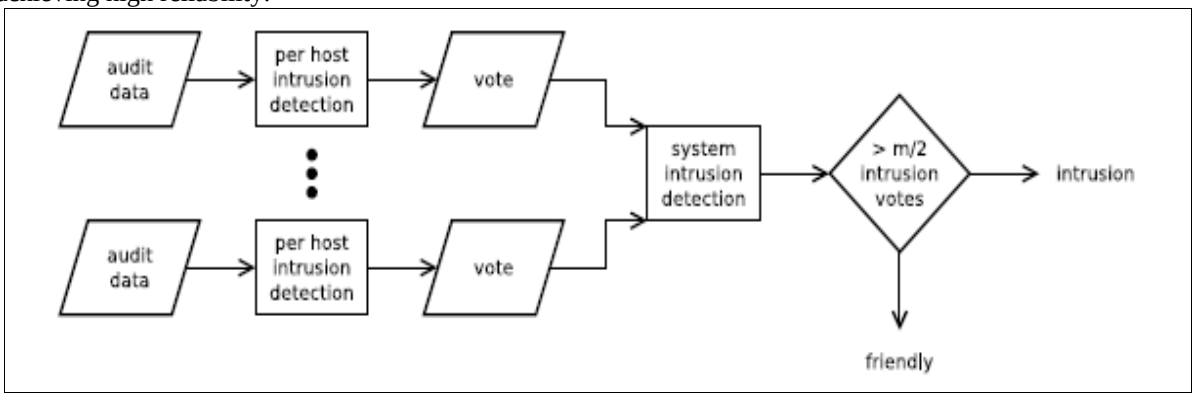

Figure 2: Combined Intrusion Detection Flow-chart

5.7 Intrusion Response

Our IDRS reacts to malicious events detected at runtime. This approach results in a smaller false negative probability, which has a positive effect of reducing the number of bad nodes in the system, and decreasing the probability of impairment security failure. However, it also results in a larger false positive

probability, which has the negative effect of reducing the number of good nodes in the system, and consequently increasing the probability of Byzantine security failure. To compensate for the negative effect, the IDRS increases the audit rate (by decreasing the intrusion detection interval) or increases the number of detectors to reduce the false positive probability at the expense of more energy consumption.

5.8 Regular Expression Technique

There are various intrusion detection systems available. Regular expressions are a formal way to describe string patterns. They provide a powerful and compact way to specify patterns in your data.

Regular expressions are a pattern matching standard for string parsing and replacement. They are used on a wide range of platforms and programming environments. Regular expressions, or *regexes* for short, are a way to match text with patterns. They are a powerful way to find and replace strings that take a defined format. For example, regular expressions can be used to parse dates, urls and email addresses, log files, configuration files, command line switches or programming scripts.

Regular expression is a sequence of the following items:

- A literal character.
- A matching character, character set, or character class.
- A repetition quantifier.
- An alternation clause.
- A subpattern grouped with parentheses.

VI. Expected Outcome And Future Work

6.1 Expected Outcome

This research will help us to develop a probability model to analyze the reliability of a cyber physical system in the presence of both malicious nodes exhibiting a range of attacker behaviors, and intrusion detection and response system for detecting and responding to malicious events at runtime. For each attacker behavior, we will try to identify the best detection strength (in terms of the detection interval and the number of detectors), and the best response strength (in terms of the per-host minimum compliance threshold for setting the false positive and negative probabilities),under which the reliability of the system may be maximized.

6.2 Future work

There are several future research directions, including (a) investigating other intrusion detection criteria (e.g., based on accumulation of deviation from good states) to improve the false negative probability without compromising the false positive probability; (b) investigating other intrusion response criteria (e.g., exponential increase of the minimum compliance threshold) other than the linear function used in the paper, and analyzing the effect on the system lifetime; (c) exploring other attack behavior models (e.g., an oracle attacker that can adjust the attacker strength depending on the detection strength to maximize security failure), and investigating the best dynamic response design to cope with such attacks; (d) developing a more elaborate model to describe the relationship between intrusion responses and attacker behaviors, and justifying such a relationship model by means of extensive empirical studies; and (e) extending the analysis to hierarchically- structured intrusion detection and response system design for a large CPS consisting of multiple enclaves each comprising heterogeneous entities subject to different operational and environment conditions and attack threats.

VII. Conclusion

The goal of this research is to design and validate resilient, energy-aware and adaptive IDS that can maximize the lifetime of CPSs in the presence of malicious attacks, as well as malicious, erroneous, partly trusted, uncertain and incomplete audit information. We investigated host IDS, system-level IDS and intrusion response designs that help move toward this goal. This research explores the development of a probability model to analyze the reliability of a cyber physical system (CPS) containing malicious nodes exhibiting a range of attacker behaviors and an intrusion detection and response system (IDRS) for detecting and responding to malicious events at runtime. For each attacker behavior, we tends to identify the best detection strength (in terms of the detection interval and the number of detectors), and the best response strength (in terms of the per-host minimum compliance threshold for setting the false positive and negative probabilities), under which the reliability of the system may be maximized.

References

Journal Papers:

[1]. Bradley, T.(n.d) "Introduction To Intrusion Detection System(IDS)" International Journal of Computer Science & technology VOL.2,NO.3, March-2011.

Theses:

[2]. M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, *"Security challenges in next generation cyber physical systems,"* in Beyond SCADA: Networked Embedded Control for Cyber Physical Systems. Pittsburgh, PA, USA: NSF TRUST Science and Technology Center, NOV. 2006.

[3]. Robert R. Mitchell III, Eric Cronin, Micah Sherr, Matt Blaze, Zachary Ives, Insup Lee *"Design and Analysis of Intrusion Detection Protocols in Cyber Physical Systems"* Institute Of Electrical And Electronics Engineers Of Computer Security, Vol.10,NO.2, November-2010.

[4]. Alvaro A. C´ardenas, Saurabh Aminy, Bruno Sinopoliz, Annarita Giani Adrian Perrigz Shankar Sastry *"Challenges for Securing Cyber Physical Systems"* VOL.25,NO.12,September-2010

Proceedings Paper

[5]. Robert Mitchell and Ing-Ray Chen, Member, IEEE *"*Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems" IEEE TRANSACTIONS ON RELIABILITY, VOL. 62, NO. 1, MARCH 2013.

[6]. L.Ying, Z. Yan, and O. Yang-jia. "The Design and Implementation of Host-Based Intrusion Detection System" In Third International Symposium on Intelligent Information Technology and Security Informatics, pages 595–598, Jinggangshan, China, April 2010.