Inspiring the
Leading
Teachnologies

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

ElysiumPRO
Final Year Projects

Cyber Security

Titles & Abstract

2023-2024

elysiumpro.in

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_001

An AI-Driven VM Threat Prediction Model for Multi-Risks Analysis-Based Cloud Cybersecurity

Cloud virtualization technology, ingrained with physical resource sharing, prompts cybersecurity threats on users' virtual machines (VMs) due to the presence of inevitable vulnerabilities on the offsite servers. Contrary to the existing works which concentrated on reducing resource sharing and encryption/decryption of data before transfer for improving cybersecurity which raises computational cost overhead, the proposed model operates diversely for efficiently serving the same purpose. This article proposes a novel multiple risks analysis-based VM threat prediction model (MR-TPM) to secure computational data and minimize adversary breaches by proactively estimating the VMs threats. It considers multiple cybersecurity risk factors associated with the configuration and management of VMs, along with analysis of users' behavior. All these threat factors are quantified for the generation of respective risk score values and fed as input into a machine learning-based classifier to estimate the probability of threat for each VM. The performance of MR-TPM is evaluated using benchmark Google Cluster and OpenNebula VM threat traces.

EPRO_BC_002

Guest Editorial Security, Reliability, and Safety in IoT-Enabled Maritime Transportation Systems

The Internet of Things (IoT) is delivering solutions with improved efficiency and security, and providing better productivity in manufacturing, retail, and other sectors. Maritime Transportation Systems (MTSs) is currently adopting the IoT to move toward a digitalized, data-driven world with increased efficiency and lower costs, and creating new revenue opportunities. Integration of the IoT also enables real-time tracking of shipments, improved efficiency in cargo handling, pre-emptive maintenance, route optimization, reduced fuel consumption, and improved safety in maritime transportation systems. With IoT technology expanding and evolving rapidly, more applications are predicted to assist and improve all aspects of MTSs, making them hassle-free and safe

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_003

Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree

Cyber-attacks pose increasing challenges in precisely detecting intrusions, risking data confidentiality, integrity, and availability. This review paper presents recent IDS taxonomy, a comprehensive review of intrusion detection techniques, and commonly used datasets for evaluation. It discusses evasion techniques employed by attackers and the challenges in combating them to enhance network security. Researchers strive to improve IDS by accurately detecting intruders, reducing false positives, and identifying new threats. Machine learning (ML) and deep learning (DL) techniques are adopted in IDS systems, showing potential in efficiently detecting intruders across networks. The paper explores the latest trends and advancements in ML and DL-based network intrusion detection systems (NIDS), including methodology, evaluation metrics, and dataset selection. It emphasizes research obstacles and proposes a future research model to address weaknesses in the methodologies.

EPRO_CYS_004

Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies

Artificial intelligence algorithms have a leading role in the field of cybersecurity and attack detection, being able to present better results in some scenarios than classic intrusion detection systems such as Snort or Suricata. In this sense, this research focuses on the evaluation of characteristics for different well-established Machine Leaning algorithms commonly applied to IDS scenarios. To do this, a categorization for cybersecurity data sets that groups its records into several groups is first considered. Making use of this division, this work seeks to determine which neural network model (multilayer or recurrent), activation function, and learning algorithm yield higher accuracy values, depending on the group of data. Finally, the results are used to determine which group of data from a cybersecurity data set are more relevant and representative for the intrusion detection, and the most suitable configuration of Machine Learning algorithm to decrease the computational load of the system

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_005

Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree

Internet of Things (IoT) devices that are purchased from a variety of suppliers & installed in significant amounts are subject to increasing cybersecurity vulnerabilities. Consequently, it has become more crucial for telecom companies to control such devices. Current monitoring systems for communication analyze data through specialized speed on networking devices or thorough protocol analysis in programs, but these methods can be difficult, costly, rigid, and unable to scale. Using the SDN architecture together with ML, we harness the advantages of configurable motion-relied telemetry with adaptable information driven designs to control IoT gadgets depending on their system behavior in this article. Our 3 results are as follows: (1) Over the course of a half year period, we examine the network traffic patterns of 17 individual customer IoT devices in the laboratory as well as recognize a collection of traffic patterns (for every device) for whom the period characteristics tabulated at numerous timeframes (from a minute to an hour) characterize the connectivity.

EPRO_CYS_006

Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security

Cyber Supply Chain (CSC) system is complex which involves different sub-systems performing various tasks. Security in supply chain is challenging due to the inherent vulnerabilities and threats from any part of the system which can be exploited at any point within the supply chain. This can cause a severe disruption on the overall business continuity. Therefore, it is paramount important to understand and predicate the threats so that organization can undertake necessary control measures for the supply chain security. Cyber Threat Intelligence (CTI) provides an intelligence analysis to discover unknown to known threats using various properties including threat actor skill and motivation, Tactics, Techniques, and Procedure (TT and P), and Indicator of Compromise (IoC). This paper aims to analyse and predicate threats to improve cyber supply chain security. We have applied Cyber Threat Intelligence (CTI) with Machine Learning (ML) techniques to analyse and predict the threats based on the CTI properties.

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_007

Towards secured online monitoring for Digitalized GIS Against Cyber-Attacks Based on IoT and Machine Learning

Developing tools that help us understand and analyze the effects of cyber attacks on physical assets is necessary in order to detect and prevent harmful consequences of integrating Information and Communication Technologies (ICTs). In this paper, we review existing technologies for developing a fully virtualized cyberphysical testbed for cyber and physical data acquisition and machine learning anomaly detection. We present a testbed that uses network emulation and real industrial communication protocols to emulate the interactions of ICTs inside a wind-powered system. We use the testbed to simulate malicious cyber attacks, their effect on the physical system, and detection mechanisms for such disturbances using anomaly detection. The advantages of the presented virtualized testbed are: 1) integration of real industrial protocols, network analysis tools, and industry-leading data-engineering and machine learning tools; 2) enables a holistic analysis of cyber-physical systems by acquiring and analyzing simultaneously cyber and physical data; 3) cost effective solution for prototyping and testing that can run in a single laptop.

EPRO_CYS_008

Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System

Industrial automation and control systems (IACS) are tremendously employing supervisory control and data acquisition (SCADA) network. However, their integration into IACS is vulnerable to various cyber-attacks. In this article, we first present population extremal optimization (PEO)-based deep belief network detection method (PEO-DBN) to detect the cyber-attacks of SCADA-based IACS. In PEO-DBN method, PEO algorithm is employed to determine the DBN's parameters, including number of hidden units and the size of mini-batch and learning rate, as there is no clear knowledge to set these parameters. Then, to enhance the performance of single method for cyber-attacks detection, the ensemble learning scheme is introduced for aggregation of the proposed PEO-DBN method, called EnPEO-DBN. The proposed detection methods are evaluated on gas pipeline system dataset and water storage tank system dataset from SCADA network traffic by comparing with some existing methods. Through performance analysis, simulation results show the superiority of PEO-DBN and EnPEO-DBN

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_009

Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning

In this paper, we propose a new comprehensive realistic cyber security dataset of IoT and IIoT applications, called Edge-IIoTset, which can be used by machine learning-based intrusion detection systems in two different modes, namely, centralized and federated learning. Specifically, the dataset has been generated using a purpose built IoT/IIoT testbed with a large representative set of devices, sensors, protocols and cloud/edge configurations. The IoT data are generated from various IoT devices (more than 10 types) such as Low-cost digital sensors for sensing temperature and humidity, Ultrasonic sensor, Water level detection sensor, pH Sensor Meter, Soil Moisture sensor, Heart Rate Sensor, Flame Sensor, etc.). Furthermore, we identify and analyze fourteen attacks related to IoT and IIoT connectivity protocols, which are categorized into five threats, including, DoS/DDoS attacks, Information gathering, Man in the middle attacks, Injection attacks, and Malware attacks.

EPRO_CYS_010

Machine Learning and Deep Learning Approaches for CyberSecurity

The rapid evolution and growth of the internet through the last decades led to more concern about cyber-attacks that are continuously increasing and changing. As a result, an effective intrusion detection system was required to protect data, and the discovery of artificial intelligence's sub-fields, machine learning, and deep learning, was one of the most successful ways to address this problem. This paper reviewed intrusion detection systems and discussed what types of learning algorithms machine learning and deep learning are using to protect data from malicious behavior. It discusses recent machine learning and deep learning work with various network implementations, applications, algorithms, learning approaches, and datasets to develop an operational intrusion detection system

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_011

Data-Driven Correlation of Cyber and Physical Anomalies for Holistic System Health Monitoring

Concerns of cyber-security threats are increasingly becoming a part of everyday operations of cyber-physical systems, especially in the context of critical infrastructures. However, despite the tight integration of cyber and physical components in modern critical infrastructures, the monitoring of cyber and physical subsystems is still done separately. For successful health monitoring of such systems, a holistic approach is needed. This paper presents an approach for holistic health monitoring of cyber-physical systems based on cyber and physical anomaly detection and correlation. We provide a data-driven approach for the detection of cyber and physical anomalies based on machine learning. The benefits of the presented approach are: 1) integrated architecture that supports the acquisition and real-time analysis of both cyber and physical data; 2) a metric for holistic health monitoring that allows for differentiation between physical faults, cyber intrusion, and cyber-physical attacks. We present experimental analysis on a power-grid use case using the IEEE-33 bus model. The system was tested on several types of attacks such as network scan, Denial of Service (DOS), and malicious command injections.

EPRO_CYS_012

Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems

Securing Internet-of-Things (IoT)-enabled cyber-physical systems (CPS) can be challenging, as security solutions developed for general information/operational technology (IT/OT) systems may not be as effective in a CPS setting. Thus, this article presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS). At the first level, a decision tree combined with a novel ensemble deep representation-learning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed to facilitate attack attribution. The proposed model is evaluated using real-world data sets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_013

Cyber Intrusion Prevention for Large-Scale Semi-Supervised Deep Learning Based on Local and Non-Local Regularization

The cyber intrusion prevention model represents a new means of cyber protection with intelligent defense capability. It can not only detect intrusion behavior but also respond to such behavior in a timely manner. This study applies deep learning theory and semi-supervised clustering to cyber intrusion prevention technology. Deep learning based on deep structures represents the current development trend of neural networks. Semi supervised learning uses a large amount of unlabeled cyber traffic data and a small amount of labeled cyber traffic data to achieve cyber intrusion prevention with a low recognition error rate. Discriminative deep belief network (DDBN)-based cyber defense technology has emerged as a research hotspot in the field of cyber intrusion prevention owing to its low error rate. This paper proposes a cyber intrusion prevention technology using DDBN for large-scale semi-supervised deep learning based on local and non-local regularization to overcome the problem of high classification error rates of the cyber intrusion prevention model.

EPRO_CYS_014

A Comparative Study of Deep Learning based Named Entity Recognition Algorithms for Cybersecurity

Named Entity Recognition (NER) is important in the cybersecurity domain. It helps researchers extract cyber threat information from unstructured text sources. The extracted cyber-entities or key expressions can be used to model a cyber-attack described in an open-source text. A large number of general-purpose NER algorithms have been published that work well in text analysis. These algorithms do not perform well when applied to the cybersecurity domain. In the field of cybersecurity, the open-source text available varies greatly in complexity and under-lying structure of the sentences. General-purpose NER algorithms can misrepresent domain-specific words, such as "malicious" and "javascript". In this paper, we compare the recent deep learning-based NER algorithms on a cybersecurity dataset. We created a cybersecurity dataset collected from various sources, including "Microsoft Security Bulletin" and "Adobe Security Updates". Some of these approaches proposed in literature were not used for Cybersecurity. Others are innovations proposed by us. This comparative study helps us identify the NER algorithms that are robust and can work well in sentences taken from a large number of cybersecurity sources. We tabulate their performance on the test set and identify the best NER algorithm for a cybersecurity corpus. We also discuss the different embedding strategies that aid in the process of NER for the chosen deep learning algorithms.

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_015

Using Deep Learning For Assessing Cybersecurity Economic Risks In Virtual Power Plants

This paper presents an assessment procedure for evaluating economic risks in Virtual Power Plants (VPPs) using two deep learning techniques, viz., Naïve Bayes algorithm and J48 bagging tree model. A comprehensive matrix of cybersecurity economic assessment based on threats, motives, impacts, challenges and economic impacts is provided in this paper. Cybersecurity risk quantification and their measurement and Cyber risk mitigation frameworks are also dealt with in this paper. Our cybersecurity risk Return On Security Investment (ROSI) model employs 9-parameters, while our dataset collection is classified into 11 types of attack profiles. The results obtained from Naïve Bayes classifier and CRQ using J48 bagging tree model yield a predictor accuracy of 82%, while the classifier correctly classifies instances in Naïve Bayes with a Receiver-Operator Characteristic (ROC) area of 0.940 indicating the good classification of the sampled data; the prediction rate is 94.2% for the CRQ-J48.

EPRO_CYS_016

AI meets Cybersecurity

Summary form only given, as follows. The complete presentation was not made available for publication as part of the conference proceedings. With the growing processing power of computing systems and the increasing availability of massive datasets, along with novel concepts and architectures for deep learning, AI algorithms have led to major breakthroughs in many different areas ioncluding cybersecurity. Nowadays AI has become one of the key enablers to studying and addressing cybersecurity-relevant problems at large in several application domains such as for intrusion detetction, malware detection and spam detection. However, it is important to consider that AI can be used also by attackers to continually improve their techniques and refine their offensive capabilities. Studying the effectiveness of AI is thus critical to ensure modern cybersecurity equipped to face the emerging threats allowed by malicious uses of AI. In this talk I will showcase several examples of recent progress in applying AI into cyber-threat detection problems and will provide a glimpse into exciting future directions that promise to have a profound impact on cybersecurity.

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_017

tCLD-Net: A Transfer Learning Internet Encrypted Traffic Classification Scheme Based on Convolution Neural Network and Long Short-Term Memory Network

The Internet is about to enter the era of full encryption. Traditional traffic classification methods only work well in non-encrypted environments. How to identify the specific types of network encrypted traffic in an encrypted environment without decryption is one of the foundations for maintaining cyberspace security. Traffic classification based on machine learning relies heavily on the prior knowledge of experts to construct feature sets. Although traffic classification based on deep learning can reduce human intervention, it requires a large amount of labeled data for parameter determination. This paper proposes a tCLD-Net model that combines transfer learning and deep learning. It can be trained on a small amount of labeled data to distinguish network encrypted traffic with a high accuracy. It pre-trains a CLD-Net model in the source domain data set, and fixes the parameters of the convolutional neural network module in it, and trains and tests it in the target domain data set.

EPRO_CYS_018

Deep learning based attack detection for cyber-physical system security

In recent years, there has been an increasing demand for computing devices in cyber-physical systems (CPS), which include smart manufacturing, air intelligent transportation, critical infrastructure, robotic services, and Internet of Things (IoT) infrastructure. Field devices, on the other hand, such as sensors and actuators, which are frequently used for real-time monitoring and prediction, send a large amount of data through the network and communication layers. The CPS is vulnerable to major cybersecurity attacks. To overcome this, there's a need for new deep learning (DL) techniques that can investigate, detect, and respond to changes in such attacks. In this paper, we proposed a DL model for cyber security attack detection in the CPS based on long-short term memory (LSTM). Moreover, the model has been evaluated using real-world datasets from Industrial Control System (ICS) datasets of gas pipelines, which consist of seven attack types with 19 features. The results of the experiment show that the proposed model achieved an accuracy of 98.22% after validation. The paper also presents a recommendation for potential future investigation

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_019

An Intelligent Intrusion Detection System for Smart Consumer Electronics Network

The technological advancements of Internet of Things (IoT) has revolutionized traditional Consumer Electronics (CE) into next-generation CE with higher connectivity and intelligence. This connectivity among sensors, actuators, appliances, and other consumer devices enables improved data availability, and provides automatic control in CE network. However, due to the diversity, decentralization, and increase in the number of CE devices the data traffic has increased exponentially. Moreover, the traditional static network infrastructure-based approaches need manual configuration and exclusive management of CE devices. Motivated from the aforementioned challenges, this article presents a novel Software-Defined Networking (SDN)- orchestrated Deep Learning (DL) approach to design an intelligent Intrusion Detection System (IDS) for smart CE network. In this approach, we have first considered SDN architecture as a promising solution that enables reconfiguration over static network infrastructure and handles the distributed architecture of smart CE network by separating the control planes and data planes.

EPRO_CYS_020

Trust–SIoT: Towards Trustworthy ObjectClassification in the Social Internet of Things

The recent emergence of the promising paradigm of the Social Internet of Things (SIoT) is a result of an intelligent amalgamation of the social networking concepts with the Internet of Things (IoT) objects (also referred to as "things") in an attempt to unravel the challenges of network discovery, navigability, and service composition. This is realized by facilitating the IoT objects to socialize with one another, i.e., similar to the social interactions amongst the human beings. A fundamental issue that mandates careful attention is to thus establish, and over time, maintain trustworthy relationships amongst these IoT objects. Therefore, a trust framework for SIoT must include object-object interactions, the aspects of social relationships, credible recommendations, etc., however, the existing literature has only focused on some aspects of trust by primarily relying on the conventional approaches that govern linear relationships between input and output. In this paper, an artificial neural network-based trust framework, Trust-SIoT, has been envisaged for identifying the complex non-linear relationships between input and output in a bid to classify the trustworthy objects. Moreover, Trust SIoT has been designed for capturing a number of key trust metrics as input, i.e., direct trust by integrating both current and past interactions, reliability, and benevolence of an object, credible recommendations, and the degree of relationship by employing a knowledge graph embedding.

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_021

IdenMultiSig: Identity-Based Decentralized Multi-Signature in Internet of Things

Most devices in the Internet of Things (IoT) work on unsafe networks and are constrained by limited computing, power, and storage resources. Since the existing centralized signature schemes cannot address the challenges to security and efficiency in IoT identification, this article proposes IdenMultiSig, a decentralized multi-signature protocol that combines identity-based signature (IBS) with Schnorr scheme under discrete logarithms on elliptic curves. First, to solve the problem of offline or faulty devices under unstable networks, we introduce a novel improvement of the existing Schnorr scheme by introducing a threshold Merkle tree for the verification with only m valid signatures among n participants (m – n tree), while hiding the real identity to protect the data security and privacy of IoT nodes.

EPRO_CYS_022

Wireless Distributed Consensus in Vehicle to Vehicle Networks for Autonomous Driving

Vital societal and industrial autonomous components are increasingly interconnected through communication networks to complete critical tasks cooperatively. However, as the reliability and trust requirements for connected autonomous systems continue to grow, the centralized communication and decision approaches that are in use today are reaching their limits. Focusing on autonomous driving applications, this paper proposes a resilient and trustworthy framework on wireless distributed consensus networks, where the communication links are less reliable or are even in the presence of incorrect local sensor readings/decisions. To accomplish that, a novel three stages consensus mechanism is proposed based on the practical Byzantine fault tolerance (PBFT), where the veto collection and gossip stages are designed to meet the stringent and complex requirements for a vehicle's maneuvers. A plan tree synthesis is also proposed to make consensus on a series of decisions while adopting network

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_023

Robust Adversarial Attacks Detection based on Explainable Deep Reinforcement Learning for UAV Guidance and Planning

The dangers of adversarial attacks on Uncrewed Aerial Vehicle (UAV) agents operating in public are increasing. Adopting AI-based techniques and, more specifically, Deep Learning (DL) approaches to control and guide these UAVs can be beneficial in terms of performance but can add concerns regarding the safety of those techniques and their vulnerability against adversarial attacks. Confusion in the agent's decisionmaking process caused by these attacks can seriously affect the safety of the UAV. This paper proposes an innovative approach based on the explainability of DL methods to build an efficient detector that will protect these DL schemes and the UAVs adopting them from attacks. The agent adopts a Deep Reinforcement Learning (DRL) scheme for guidance and planning. The agent is trained with a Deep Deterministic Policy Gradient (DDPG) with Prioritised Experience Replay (PER) DRL scheme that utilises Artificial Potential Field (APF) to improve training times and obstacle avoidance performance.

EPRO_CYS_024

Secure Deep Learning in Defense in Deep-Learning-as-a-Service Computing Systems in Digital Twins

While Digital Twins (DTs) bring convenience to city managers, they also generate new challenges to city network security. Currently, cyberspace security becomes increasingly complicated. Intrusion detection and Deep Learning (DL) are combined with shunning security threats in service computing systems and improving network defense capabilities. DTs can be applied to network security. Peoples understanding of cyberspace security can be improved using DTs to digitally define, model, and display the network environment and security status. The intrusion detection data are optimized based on DL technology, and a network intrusion detection algorithm integrated with Deep Neural Network (DNN) model is proposed. In the cloud service system, a trust model based on Keyed-Hashing-based Self-Synchronization (KHSS) is introduced. This model predicts the security state and detects attacks according to existing malicious attacks, ensuring the network security defense systems regular operation. Finally, simulation experiments verify the Deep Belief Networks (DBN) models feasibility and the cloud trust model. The DBN algorithm proposed improves the correct detection rate of unknown samples by 4.05% compared with the Support Vector Machine (SVM) algorithm.

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_025

An Underestimated Cybersecurity Problem: Quick-Impact Time Synchronization Attacks and A Fast-Triggered Detection Method

For cybersecurity concerns in smart girds, this paper has focused on the vulnerability analysis and defense technique against the Time Synchronization Attack (TSA). This kind of attack can spoof satellite-signal-based time synchronization processes that are widely utilized in modern power systems. A quick-impact TSA experiment is presented in this paper, based on live satellite signals and a commercial time server used in current smart grids. Experiment results are alarming. Intolerable timing errors have been imposed on the server within a few tens of seconds, and it hasn't reported any alarms. So a new cybersecurity concern for distributed power systems is revealed: stealthy TSAs must be detected at the early stage due to their quick impacts, yet current studies have underestimated this problem. In response to this potential threat, a fast-triggered detection method is proposed in this paper. It is named the Rapid Detection of Signal Distortions (RDSD) and can detect early stage signal distortions caused by TSAs at the beginning. Apart from this ability, we have also verified, via simulations and real-world comparative experiments, that the proposed method can provide improved detection and false alarm rejection capacity compared with existing methods of this type.

EPRO_CYS_026

Cyber-resilient Automatic Generation Control for Systems of AC Microgrids

In this paper we propose a co-design of the secondary frequency regulation in systems of AC microgrids and its cyber security solutions. We term the secondary frequency regulator a Micro-Automatic Generation Control (μAGC) for highlighting its same functionality as the AGC in bulk power systems. We identify sensory challenges and cyber threats facing the μAGC. To address the sensory challenges, we introduce a new microgrid model by exploiting the rank-one deficiency property of microgrid dynamics. This model is used to pose an optimal μAGC control problem that is easily implemented, because it does not require fast frequency measurements. An end-to-end cyber security solution to the False Data Injection (FDI) attack detection and mitigation is developed for the proposed μAGC. The front-end barrier of applying off-the-shelf algorithms for cyber attack detection is removed by introducing a data-driven modeling approach.

CYBER SECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

EPRO_CYS_027

Identifying and Protecting Cyber-Physical Systems' Influential Devices for Sustainable Cybersecurity

For sustainable cyber-physical systems (CPS) security, proactive measures to cybersecurity need to be implemented instead of reactive measures. Towards this, we introduce in this paper a proactive methodology implemented in a system called IDI_CPS. It is based on the observation that CPS devices that have LAN-based network sharing (e.g., via Wi-Fi connections) need first to be clustered using some clustering criterion. Then, the influential and central devices in these clusters need to be identified to pay more attention to their file sharing. These influential devices may have network sharing with devices at the WAN level. Therefore, the influential devices at the WAN level that have network sharing with the influential devices in the clusters need also to be identified to pay more attention to their file sharing. We propose novel techniques for: (1) clustering the devices that have LAN-based network sharing using k-clique modeling, (2) employing clustering coefficient-based techniques for identifying the most influential device in each cluster, and (3) employing Independent Cascades model-based techniques for identifying the influential devices at the WAN level that have network sharing with the influential devices in the clusters. We experimentally evaluated our proposed system IDI_CPS and compared it with four comparable methods. Results showed marked improvement.

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

50K+
Projects Reached

25+
Years of Experience

24/7
Desk Support

25+ Years of Experience | Automated Services | 24/7 Desk Support
Advanced Technologies and Tools | Legitimate Members of all Journals
Quality Product Training | Industry Exposure

(+91) 99447 93398

#229, First Floor, A Block, Elysium Campus,
Church Rd, Anna Nagar, Madurai,
Tamil Nadu 625020

elysiumpro.in