Generative Adversarial Networks Based Cognitive Feedback Analytics System for Integrated Cyber-Physical System and Industrial Iot Networks

Kamal Upreti
Inderprastha Engineering College

Mohammad Haider Syed
Saudi Electronic University

Mohammad Shabbir Alam
Jazan University

Adi Alhudhaif
Prince Sattam bin Abdulaziz University

Mohammed Shuaib
Jazan University

A K Sharma (✉ drarvindkumarsharma@gmail.com)
Career Point University

Research Article

Keywords: Generative adversarial networks (GAN), Cyber-Physical Production Systems (CPPS), Denial-of-Service, Cognitive feedback.

Posted Date: September 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-924288/v1

GENERATIVE ADVERSARIAL NETWORKS BASED COGNITIVE FEEDBACK ANALYTICS SYSTEM FOR INTEGRATED CYBER-PHYSICAL SYSTEM AND INDUSTRIAL IOT NETWORKS

[1]Dr. Kamal Upreti, [2]Mohammad Haider Syed, [3]Mohammad Shabbir Alam, [4]Adi Alhudhaif,
[5]Mohammed Shuaib,[6]Dr. Arvind K. Sharma

[1]Department of Information & Technology, Inderprastha Engineering College, Ghaziabad, India,
kamalupreti1989@gmail.com
[2]College of Computing and Informatics, Saudi Electronic University, KSA,
m.haider@seu.edu.sa
[3]Lecturer, Department of Computer Science, College of computer science and Information Technology, Jazan University, Kingdom of Saudi Arabia.
amushabbir@gmail.com
[4]Department of Computer Science, College of Computer Engineering and Sciences in Al-kharj, Prince Sattam bin Abdulaziz University, P.O. Box 151, Al-kharj 11942, Saudi Arabia
a.alhudhaif@psau.edu.sa
[5]College of Computer Science & IT, Jazan University, KSA
talkshuaib@gmail.com
[6]Dept. of CSI, University of Kota, Rajasthan-India
drarvindkumarsharma@gmail.com

Abstract:
In the modern era of technologies, the internet grows in the advancement of our day-to-day life like automation devices. The devices to set up industries with integrated cyber-physical systems and industrial IoT applications. Generative adversarial networks (GAN) can generate Cognitive feedback analysis with various data for both generator and discriminator in a supervised model. Neural networks are used for artificial intelligence algorithms, but in adversarial networks, feedback analytics is analyzed with the significance of data. The modern age of intelligent manufacturing will indeed be ushered in by Cyber-Physical Production Systems (CPPS). However, because of the connections between the virtual and physical worlds, CPPS would be subject to cross-domain assaults. Against Denial-of-Service (DoS) threats, this paper concentrates on complex performance feedback management of Cyber-Physical Systems (CPS). To begin, a swapping system modelling approach for the complex response feedback CPS is provided by analyzing the distinct effects of DoS assaults on the sensor-controller (S-C) and controller-to-actuator (C-A) channels, accordingly. Given the difference in bandwidth between the dual channels and the accused's energy cap, it is reasonable to conclude that an offender can only jam a single communication stream at a point and also that the possible number of successive DoS attacks is limited. Second, using a packet-based transfer scheme, a nested switching paradigm is built on the foundation of the switching mechanism, considering both the spatial heterogeneity and the temporal durability of DoS attacks. The probability of discriminator gets analyzed feedback data to check whether actual data or fake data is sampled, and it is generated. Cognitive feedback supports genetic algorithms to sample the feedback data in a system for advanced technologies.

Keywords: Generative adversarial networks (GAN), Cyber-Physical Production Systems (CPPS), Denial-of-Service, Cognitive feedback.

I. INTRODUCTION

The German government processes the cyber-physical system for manufacturing small enterprises to artificial intelligence in the advanced industrial revolution. It was introduced by a workshop held in the United States. e. a cyber system is a system that consists of entities with computation and connection around the physical world. The industrial physical world provides data on a network based on an application built for health care industries, intelligent city transportation, and intelligent feature of area grid. The revolution of a new era in technologies for integrated cyber-physical systems and industrial IoT networks. The various neural networks compiled out with cognitive feedback systems for manufacturing industries in various applications of automation devices. The generative adversarial networks (GAN) are the most exciting idea in the last ten years in machine learning, as stated by Yann LeGunn, director of Facebook AI. The main two components of general adversarial networks are generator and discriminator. The generator needs to fetch the data for distribution. The discriminator would estimate the probability of cognitive feedback analytics system that samples received feedback data rather than initial data for CPS and IoT. Figure 1 shows the integration model of the Cyber-Physical System with IoT.

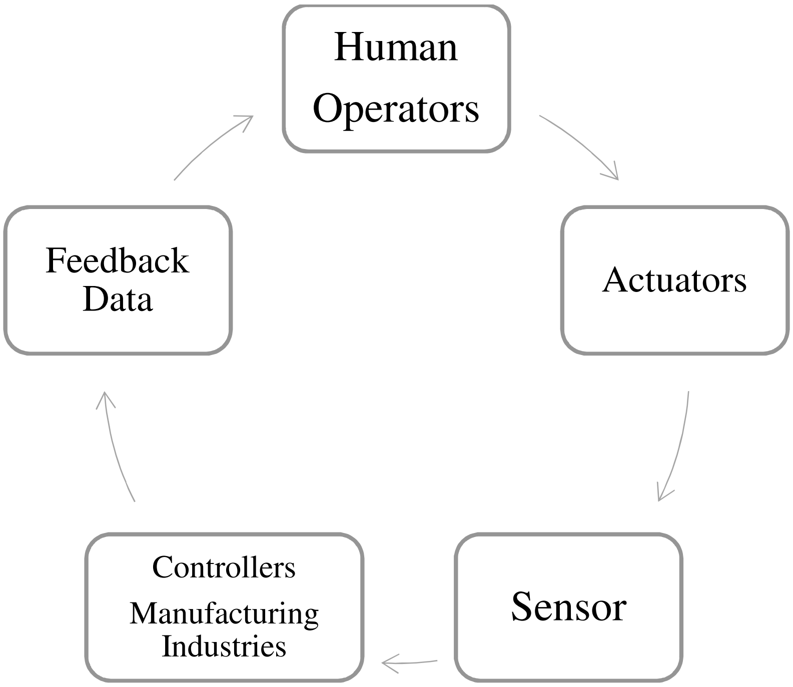

Figure 1: Integrated Cyber-Physical System with IoT.

Cyber-Physical Systems (CPS), also defined as Cyber-Physical Production Systems (CPPS), plays a significant role in the 4th industrial advancement [1]. CPPS is a collection of sub-systems across various cybersecurity realms that are linked together by communication networks. Utilizing CPPS would further help make industrial units intelligent and dynamic because of the close relationships among the cyber and physical worlds, and CPPS could have cross-domain limitations. Side-channel attacks and kinetic-cyber attacks [2] are two forms of cross-domain vulnerability achievements. Kinetic cyber-attacks are cyber-based threats that specifically affect the physical realm by compromising CPS credibility or reliability [3]. Side-channel attacks are data theft attempts that observe outputs from the physical world to steal sensitive information from the digital realm [4& 5]. More minor vulnerabilities that target secrecy, honesty, and availability can be used in all forms of attacks. The infamous Stuxnet worm threats cause physical harm in an Iranian nuclear plant over 1,000 centrifuges [6]. A cyber-attack includes attackers with a huge impairment to the blast furnace on a German Steel Mill [7] in a kinetic-cyber-attacks.

Currently, analysis into the controlled defence of CPS faces communication attacks focuses on Security threats, replay attacks, fake data intrusion, and so on. Cyber attacks are most dangerous and straightforward to carry out since they transmit a vast volume of data across the network. The network is insufficient to react to regular service requests because it is ready to process this insignificant information. The system's reliability is ensured under Security threats of unpredictable durations by correctly designing closed-loop poles. An optimal control strategy is determined when the DoS attacks are encountered in a Markov process model [8]. In [9], a DoS attack framework based on an attack method is developed to improve the mean covariance tracing of the Kalman evaluator from the victim's perspective.

The modern Internet of Things (IoT) model moves technical fields into a framework where virtually all can be linked and handled in the virtual environment, introducing a unique layer of communication and information technology that considers access for everyone at all times and everywhere [10]. As a result, diversity, optimization, pervasive data sharing via proximity wireless technology, energy-optimized approaches, localization and monitoring capability, self-organization features, semantic interoperability, and database management are key device features supporting IoT network technology [11]. Although the closed-loop connection of physical devices well with the internet necessitates new methods to prevent device failure induced by inappropriate information operation, the relationship between control systems and IoT is highly delicate. Conventional feedback control systems presume deterministic and secure communication.

However, certain control implementations are conducted over the internet in a management role. [12]. Control theory has obstacles that must be solved as study covering many areas of technical expertise progresses. The non - deterministic systems control latency and jitter, cyber-protection, bandwidth, physical security, interoperable hardware, adaptor sensors, and template issues [13]. Several of the obstacles experienced by IoT, including latency and jitter, are solved by implementing Network Control Systems [14], but still, interoperability and extensibility remain unsolved. The NCS's shared solution, defined as DNCS [15], shortens the journey up to an IoT era. However, non - deterministic internet features, interoperable and plug-and-play tools can result in unpredictable control loops.

The attack mechanisms primarily represent attackers' potential instead of the framework due to the reason to assume that current attack models can be extended directly to CPPS security research. Moreover, creating a proposed framework for CPS security examination presents fundamental research issues: • Current defence properties are usually only recommended for monitoring cyber-attacks [16]. The examination of cross-domain attacks in CPPS necessitates creating new forms of defence property that can be applied to the cyber-physical realms. • Numerous Models of Computation (MoCs) are required by the current system-level acceptance systematic model in CPPS for the cyber-physical realm [17]. A centralized device activity of importance for CPPS is needed to evaluate cross-domain protection. • Since several sub-systems communicate in the CPPS context, the elimination of information or detection systems must be carried out through multiple sub-systems. The GAN is being used to combine the IoT ecosystem with the current CPS framework for consistency and a long-term system.

LITERATURE REVIEW

Emerging CPPS modelling techniques aim to analyze the system's performance, stability, control quality, and energy efficiency. These resources disregard security via device design. The majority of current CPS security analysis, on the other hand, focuses on established deficiencies in particular positions. An ad hoc fix is recommended with patching applications and removing hardware parts without demonstrating that the restored device is no longer vulnerable [18]. A few of CPS eventually become a vital component of the CPPS as a whole.

Internet-oriented, Semantic-oriented, and Things-oriented perspectives [19] are included with the cyber-physical system. The experience layer consists of sensor devices. The network layer consists of a localized communication network. Finally, the application layer enables interface devices to reside with the application in the proposed structural model. Moreover, the enhanced five-layer architecture consists of the gateway layer and middleware layer involved in handling network connectivity and ensuring the interface among system and mesh devices are very versatile [20]. Specific layer-based architectural structures [21 & 22] in the studies, on the other side, provide more flexibility to satisfy the requirement of each program.

When the number of IoT implementations grows, so does the number of heterogeneous networking methods available, each with its own set of access networks and routing protocols. Incorporating those components, allowing for appropriated management in complex contexts, has been a significant challenge that must be addressed. In this regard, many modern IoT architecture concepts [23 & 24] often relied on Network-based software to address this issue. Network Virtualization innovation is also being built into this approach, allowing the IoT device quite versatile and also scalable [25&26]. Simultaneously, a study has been carried to expand SDN-based frameworks to an appropriate controller network [27]. Innovative manufacturing industries [28] are the most exciting implementations of SDN networks for IoT.

The demand for IoT systems, including quicker response times and better service efficiency, has resulted in modern edge computing techniques. The IoT tool is served as the foundation for specific architectural plans for an intelligent power grid, smart transit, and innovative city developments. In this regard, research is done on IoT factors like infrastructure related to the quality, stability, and privacy concerns to determine edge technology can be integrated [29 & 30]. Implementing a process control system within closed-loop and Distributed Networked Control Systems faces an issue that is unable to be overcome by the IoT framework, even though the numerous types of IoT framework are utilized for various applications.

The stable confinement management for discontinuous-time multi-agent networks with transmission dropouts [31]. Centred on the system's robustness [32], build a stable controller. [33] created a novel Event-triggered robust monitoring technique for CPS against interruption and additive noise in the face of dual-channel asynchronous DoS attacks. Both for S-C and C-A channels, two separate event-triggering protocols have been established. When faced with transmission dropouts triggered by DoS attacks, [34] employ state-input control.

The condition of the method, on the other hand, is not necessarily quantifiable. The regulated device state is determined by utilizing a dynamic external feedback control in associated output feedback control H∞ challenges are investigated [35]. Nonlinear observer-dependent output feedback control depending on the case cause function. Even though access monitoring challenges against DoS attacks are being studied in the literature [36& 37], several issues are yet to be successfully tackled. The primary complex problem is describing the effect of systematic attacks functionality very precisely. Attack strength and limit are selected to represent the interaction among attackers and machine efficiency [38]. The proper requirements of Nash equilibrium are investigated by utilizing a two-stage optimization technique. Nevertheless, in the presence of intellectual threats, the device must choose an optimum prediction limit based on threat rate but can still effectively mitigate transmission dropouts caused by DoS attacks. [39] Explore dynamic monitoring using the systematic switching approach and suggest a hybrid mathematical paradigm where the controller switches depending on the cyber attacker and the defender's conflicting results. Moreover, the classification technique does not consider the effect of DoS systematic attacks over various contact networks. The goal is to develop an increased performance feedback controller to address a DoS attacks issue for cyber-physical systems and prevent the length of DoS attacks by the switching subsystems categorization based on the features of persistent DoS attacks. The controller is usually programmed to optimize the Cyber-Physical System during DoS attacks using a sequence of expected potential control inputs.

II. SYSTEM MODEL

The proposed Generative Adversarial Networks (GAN) is applicable in many contemporary applications with different structural frameworks such as variant data types with the fully connected networks, generating image features with Convolutional Neural Network, and sequence data type recurrent network model. The layout of the GAN model is shown in Figure 2. The proposed algorithmic approach is involved in analyzing input data by achieving the accelerated growth that has emphasized Artificial Intelligence. In specific, systematic models are classified as conditional GANs and unconditional GANs. The generator and discriminator in the GAN model are influenced to validate the input data. Semi-supervised computing, image extraction, image capturing, feedback data collection, software optimization, and forecasting are a few contemporaneous applications of Generative Adversarial Networks (GAN).

Many sub-systems make up a standard Cyber-Physical Protection System (CPPS) layout. The elements in every sub-system's cyber and physical realm are linked based on signal and energy flows, whereas signal and energy flows can exist within sub-systems. The proposed model enables interaction among the different flows within an individual sub-system or over multiple sub-systems. This can be attained by implementing the Conditional Generative Adversarial Model (CGAN). In the CPPS design phase, the time required for signal and energy flows is estimated depending on the unique device design. The cyber and physical realm are attained using various nodes, whereas the energy and signal transfer among distinct nodes are obtained using edges. The unique pattern in the developed CPPS is utilized to display all of the possible flow and also enable us to derive the flow pairs. The CGAN generates every individual pair to the proposed model. Provided information about every single flow deduce a maximum level of probability distribution means that enables a close connection among the two flows. To achieve a security standpoint, the interaction and distribution in between different flows are enhanced. Depending on the security approach, the proposed CGAN systematic model produces a theoretical basis for the architecture and study of CPPS that opposes cross-domain threats at the device level. The enhancement of CGAN-based security for Cyber-Physical Protection System (CPPS) is an integrated IoT network facility.

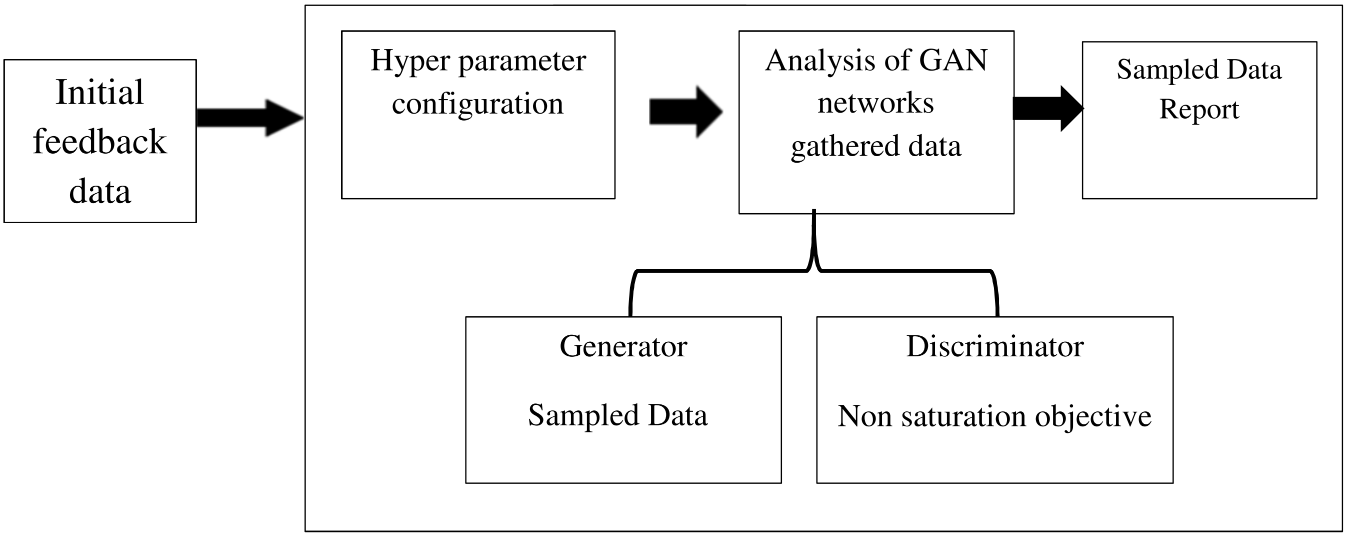

Figure 2: Layout of generative Adversarial Networks.

The proposed CGAN system model consists of a two-step approach for generating and resolve security analysis with a tool for CPPS. Graph Construction and CGAN-based Security are the two stages included in the proposed system model. The network construction algorithm uses the design time as an input along with sub-systems informational data in CPPS. Every sub-system's cyber and physical realm elements are evaluated for corresponding data of energy and signal flow within a sub-system to enhance the graphic representation from the current CPPS.

Algorithm for Security analysis:

Input: Discriminator, Generator, Noise under condition, Frequency Feature Indices, Parzen Window with Width "h".

Output: Likelihood Metrics: Average Correct Likelihood: AvgCorLike, Average Incorrect Likelihood: AvglncLike.

Step1: Initialize AvgCorLike and AvglncLike as a matrix of size batch size (N) x step size (K).

Step2: When the random condition comes under the specified condition, Correct Likelihood (CorLike)0, correct number (CorNum), Incorrect Likelihood (IncLike), and Incorrect number (IncNum) are initialized to zero.

Step3: We first produce samples $X_G$with G(Z|Cond$_i$) for each condition mark Cond$_i$.

Step4: We use the Parzen Gaussian Window approach to construct an approximate conditional distribution FtDistr = Pr(X_G^{FTIdx}|Cond$_i$) for a specified Parzen window size h and current function index Ftldx.

Step5: We generate the respective test samples within each frequency function from the test packet X_{test}, and we change two parameters based on the probability for each sample set.

Step6: The aggregate of CorLike and IncLike is then calculated based on the number of test samples per function.

Step7: Two sets of average metric values, AvgCorLike and AvglncLikeare modified with the equivalent sets of aggregated metric values, depending on the conditions.

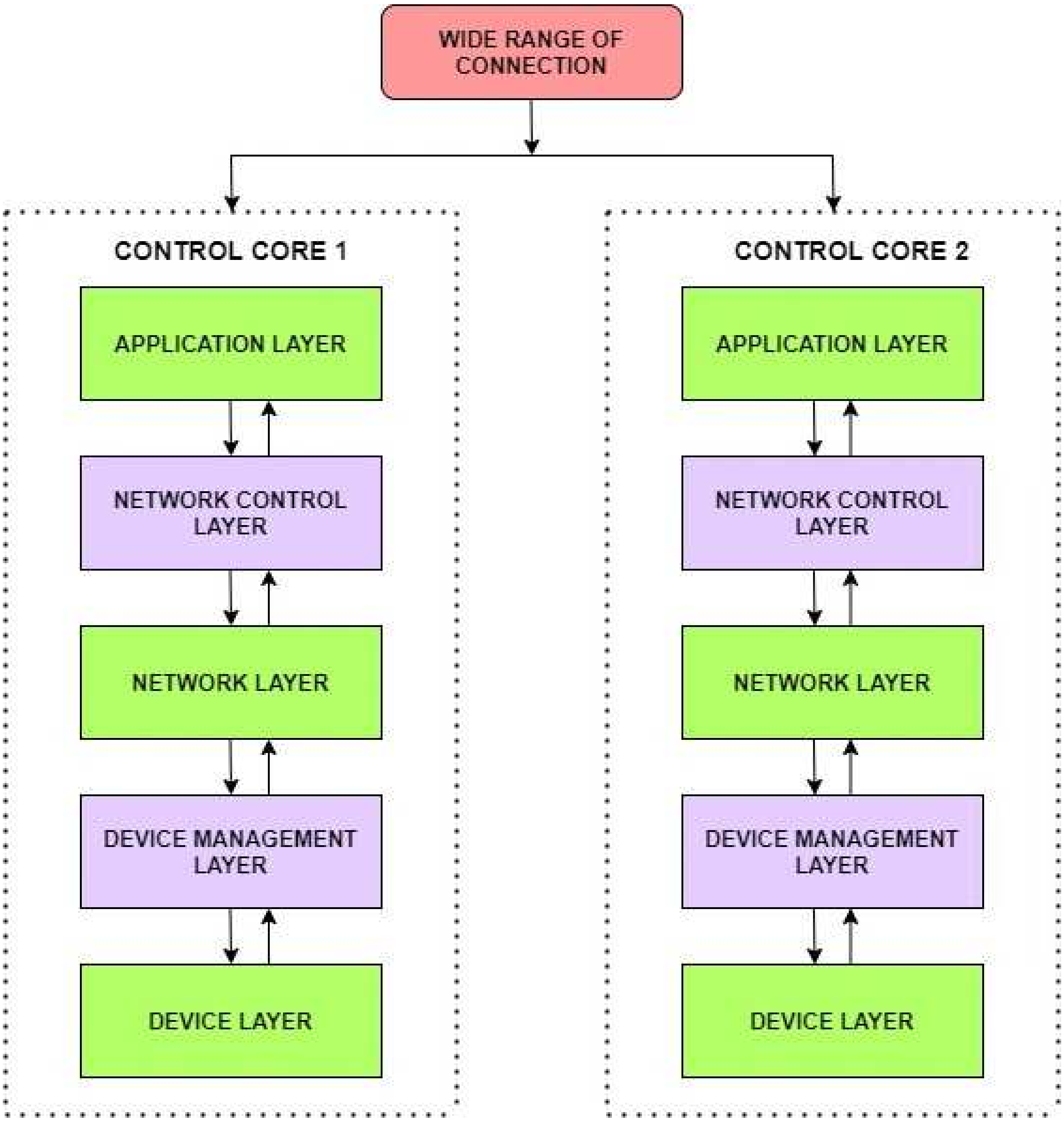

Figure 3: IoT-based distributed network control system.

To fulfil the DNCS demands satisfactorily, a layer-based structure is created considering the technical advancement forced through IoT. The IoT-based distribution network model is shown in Figure 3. The control core represents the IoT DNCS framework. The five ordered layers, namely the application layer, network layer, network control layer, device, and management layer, enable communication with each other layers based on the control core. The instruments are utilized to control systems execution by the investigators are included in the interface layer. The proposed system model utilizes controls, actuators, and sensors. The volume of data within the layer is unknown, and they are assumed to get a plug-and-play operation that is dependent or independent of a given time. As observations are needed, sensors are placed to gather the corresponding information, whereas active controllers will measure its control signals. If there is a requirement for creating an entity, actuators ensure the protection with the acquired control signals. The fundamental goal of the network management plane with the device layer is to control the devices with three tasks. Initially, the sensors are used to monitor via assessment of entering and exiting data within the device, evaluating the sensor's effectiveness and potential to conduct calculations for the investigator's creation, and making decisions based on a set of rules. The second stage is to handle the actuators by detecting the entering and exiting data within a device, assessing the actuator's accessibility and potential to quantify controlled signals for investigator's creation, and evaluating whether inter-controller switching can exist or not depending on network control specifications. The third stage is to handle the actuators, such as assessing for entering and exiting data in a system and estimate the requirement of operator preparation and assessing to shape depending on the contact network's circumstances and control specifications of members.

The Network Layer is responsible for gathering informational data from the south-bound layer and transmitting it via the connection-oriented networks. This network's centre consists of all devices and networking technology that communicates with the entities. Furthermore, this layer is responsible for route discovery to robust connectivity, improving communication among control cores. The most critical layers are the Network Control Layer that permits DNCS to function effectively in IoT configuration. The ability of the networking model is managed by providing the network layer towards the device management layer. The network control layer has the potential to self-abstract in-service management networks by permitting IoT protocol to interact with diversified devices in terms of connectivity and knowledge sharing that can reach and leave the system at varying time duration. The network control layer has the authority to determine when the device layer generates the input data or communicated via Network Layer elements and the potential to control sensors, actuators, and controllers.

The cyber-physical system (CPS) is scaled with a value of $\varepsilon_{i,n} > 1, \mu > 1$ shows that it is exponentially stable per the delay rate of $\sqrt[2(N+2)]{\rho}$. The maximum consecutive arises due to DoS attacks is existing in matrices of $P_{i,n} > 0(i \in M, n \in L)$, in which the finite set is denoted as L. If i=1, then n=0.

$$\begin{bmatrix} -P_{i,n} & \varepsilon_{i,n} K_{i,n}^{T} P_{i,n} \\ \varepsilon_{i,n} P_{i,n} K_{i,n} & -P_{i,n} \end{bmatrix} < 0 \tag{1}$$

$$P_{a,\alpha} < \mu P_{b,\beta}(\forall a, b \in M; \forall \alpha, \beta \in L) \tag{2}$$

$$\rho = \max\{\varepsilon_{i,n}^{-2}\mu \,|\, i \in M, n \in L\} < 1 \tag{3}$$

$$V_{\tau\sigma(k_t)^{(k_t)}}(k_t) = z^T(k_t) P_{\tau\sigma(k_t)^{(k_t)}} z(k_t) \tag{4}$$

Here, the Lyapunov function is denoted as $\tau\sigma(k_t)^{(k_t)}$ that are related to the nested sub-system in which $\sigma(k_t) = i(i \in M)$ and $\tau\sigma(k_t)^{(k_t)} = n(n \in L)$ whereas the sub-system in between the transmission switching points is denoted as $\tau\sigma(k_t)^{(k_t)} = n$. The sub-system of the system is given as follows,

$$z(k_{t+1}) = K_{i,n^z}(k_t)(i \in M, n \in L) \tag{5}$$

In the above equation, the Lyapunov function for a subsystem is applied and given as follows,

$$V_{i,n}(k_t) = z^T(k_t) P_{i,n^z}(k_t) \tag{6}$$

$\varepsilon_{i,n^z}^{t}(k_t) = \xi(k_t)$ is provided and the following systematic model is obtained as follows,

$$\xi(k_{t+1}) = \varepsilon_{i,n} K_{i,n} \xi(k_t) \tag{7}$$

The most appropriate Lyapunov function for the system is selected.

$$W_{i,n}(k_t) = \xi^T(k_t) P_{i,n} \xi(k_t) \tag{8}$$

The systematic approach along the trajectory with the first-order forward difference of $W_{i,n}(k_t)$ is given as follows,

$$\Delta W_{i,n}(k_t) = W_{i,n}(k_{t+1}) - W_{i,n}(k_t)$$

$$\Delta W_{i,n}(k_t) = \xi^T(k_t) \Omega_{i,n} \xi(k_t) \tag{9}$$

Here, $\Omega_{i,n} = \varepsilon_{i,n}^2 A_{i,n}^T P_{i,n} A_{i,n} - P_{i,n}$. For any non-zero $\xi(k_t), \Omega_{i,n} < 0$ which implies that $W_{i,n}(k_t) < W_{i,n}(k_0)$.

$$V_{i,n}(\mathrm{k_t}) = \varepsilon_{i,n}^{-2t}\, W_{i,n}(\mathrm{k_t})$$

$$V_{i,n}(\mathrm{k_t}) = \varepsilon_{i,n}^{-2t} V_{i,n}(\mathrm{k_0}) \tag{10}$$

The implementation of Schur complements lemma with $\Omega_{i,n} < 0$ the equivalent inequality matrix is obtained.

$$V_{\tau\sigma(\mathrm{k_t})^{(\mathrm{k_t})}}(\mathrm{k_{t+1}}) = \mathrm{z^T}(\mathrm{k_{t+1}})\mathrm{P}_{\tau\sigma(\mathrm{k_t})^{(\mathrm{k_t})}}\mathrm{z}(\mathrm{k_t}) \tag{11}$$

From equation (2) the following expression is derived,

$$\mathrm{V}_{a,\alpha} < \mu \mathrm{V}_{b,\beta}(\forall a, b \in M; \forall \alpha, \beta \epsilon L) \tag{12}$$

On considering the equation (10) and (12), the corresponding account yield is expressed as follows,

$$V_{\tau\sigma(\mathrm{k_t})^{(\mathrm{k_t})}}(\mathrm{k_t}) < \rho V_{\tau\sigma(\mathrm{k_{t-1}})^{(\mathrm{k_{t-1}})}}(\mathrm{k_{t-1}}) < \rho^2 V_{\tau\sigma(\mathrm{k_{t-2}})^{(\mathrm{k_{t-2}})}}(\mathrm{k_{t-2}}) < \cdots < \rho^t V_{\tau\sigma(\mathrm{k_0})^{(\mathrm{k_0})}}(\mathrm{k_0})$$
(13)

Here, $\rho = \max\{\varepsilon_{i,n}^{-2}\mu \,|\, i \in M, n \in L\}$.When $t \to \infty, \rho < 1$, $V_{\tau\sigma(\mathrm{k_t})^{(\mathrm{k_t})}}(\mathrm{k_t})$converges to 0. To obtain the convergence of the entire system the state sequence are considered. Thus, the relationship between the two-state sequences is given as follows,

$$\|\mathrm{z}(\mathrm{k_{j,t}})\| \leq \lambda \|\mathrm{z}(\mathrm{k_t})\| \tag{14}$$

The entire state equation converges to 0 when $t \to \infty$. Thus, the proposed system remains stable at any transmission switching rate.

For the efficient cyber-physical system transmission, the terms such as $\mathrm{t}, \mathrm{k_t}$ and $\mathrm{k_{j,t}}$ are considered as the equation is given as follows,

$$\mathrm{k_t} \leq (N+1)t \tag{15}$$

$$\mathrm{k_{j,t}} \leq (N+1)t + N \leq (N+2)t, (t \geq N) \tag{16}$$

$$\|\mathrm{z}(\mathrm{k_t})\| < \left(\sqrt[2(N+1)]{\rho}\right)^{\mathrm{k_t}} \sqrt{\left(\theta_2/\theta_1\right)}\, \|\mathrm{z}(0)\| \tag{17}$$

$$\|\mathrm{z}(\mathrm{k_{t,j}})\| < \lambda\left(\sqrt[2(N+2)]{\rho}\right)^{\mathrm{k_{t,j}}} \sqrt{\left(\theta_2/\theta_1\right)}\, \|\mathrm{z}(0)\|, (t \geq N) \tag{18}$$

The expression for inequality switching point after transmission at the varying time is given as follows,

$$\|\mathrm{z}(\mathrm{k})\| < \lambda\left(\sqrt[2(N+2)]{\rho}\right)^{\mathrm{k}} \sqrt{\left(\theta_2/\theta_1\right)}\, \|\mathrm{z}(0)\| \tag{19}$$

At N(N+1) time steps, the corresponding least packet transmission point is obtained with the transmission switching point. Thus, the cyber-physical system (CPS) is exponentially stable at finite time steps with the delay rate.

III. RESULT AND DISCUSSION

Based on the proposed model, designed to attain the various data analysis observed to be accurate data or fake data with a probability of generator and discriminator. The Generative Adversarial Networks (GAN) can transverse the feedback data with a sampled model at a supervised deep learning method. It also reverses the feedback data with a Non-saturating objective model at the rate of the deep reinforcement learning system method.

The purpose is to reduce the data loss during feedback analysis in the integrated cyber systems and artificial intelligence and improve data significance.

A higher score indicates that the proposed model has learned a stronger relationship between the featured data and the right running conditions of the motor during the first sequence. Increasing value in the second range, on the other hand, indicates that the proposed system model discovered unforeseen and perhaps unsustainable interactions between data and variables.

Freq = [freq, freq2..., freqioo], frequency values are ranging from 0 and 1. The Gaussian kernel density estimate uses a parzen frame with the width of h=0.2. As a result, frequency components are multiplied by 0.2 to yields the real likelihood. The mean value of right and inaccurate likelihood is shown in Figure 4. The positive probability values change as the number of iterations increases. This demonstrates that the generator can study the standard acoustic emissions distribution based on signal flows with accuracy. We have been using the protection analysis algorithm to quantify the emission with the mean correct and incorrect likelihoods acquired with three parameters by utilizing the CGAN generator concerning the density function.

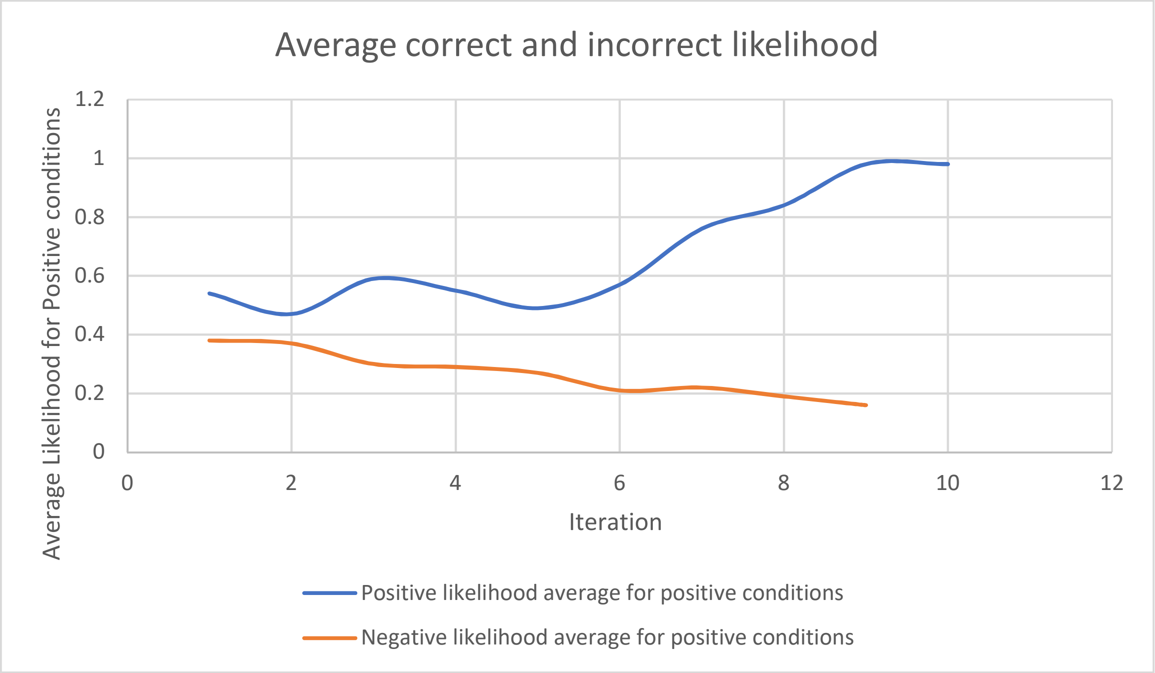

Figure 4: Average correct and incorrect likelihood for iteration with h=0.2.

The existence of the Z-motor activity in the G/M-code is best estimated by an intruder rather than other situations, as seen in Figures 5 and 6, and it is represented with X or Y movement of the motor. Furthermore, if a user has to build an integrity and accessibility attack prediction model to identify attacks on individual elements of X, Y, or Z motor via side channels, the proposed CGAN model would enable the user to predict the output of this model.

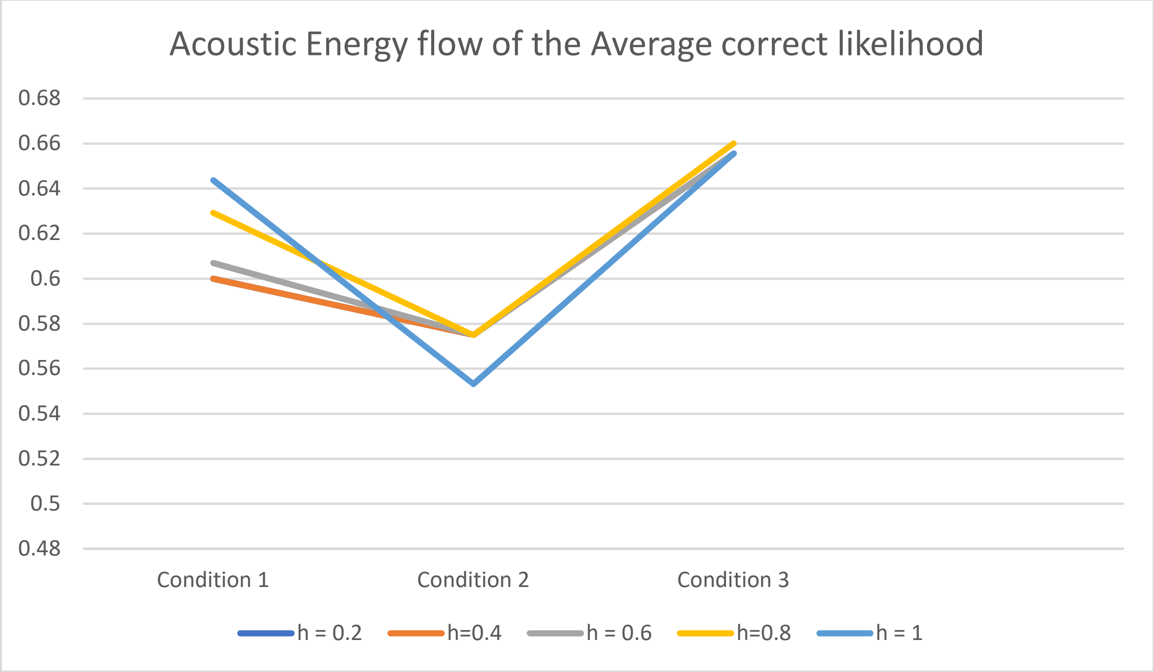

Figure 5: Acoustic Energy flow of the Average correct likelihood.

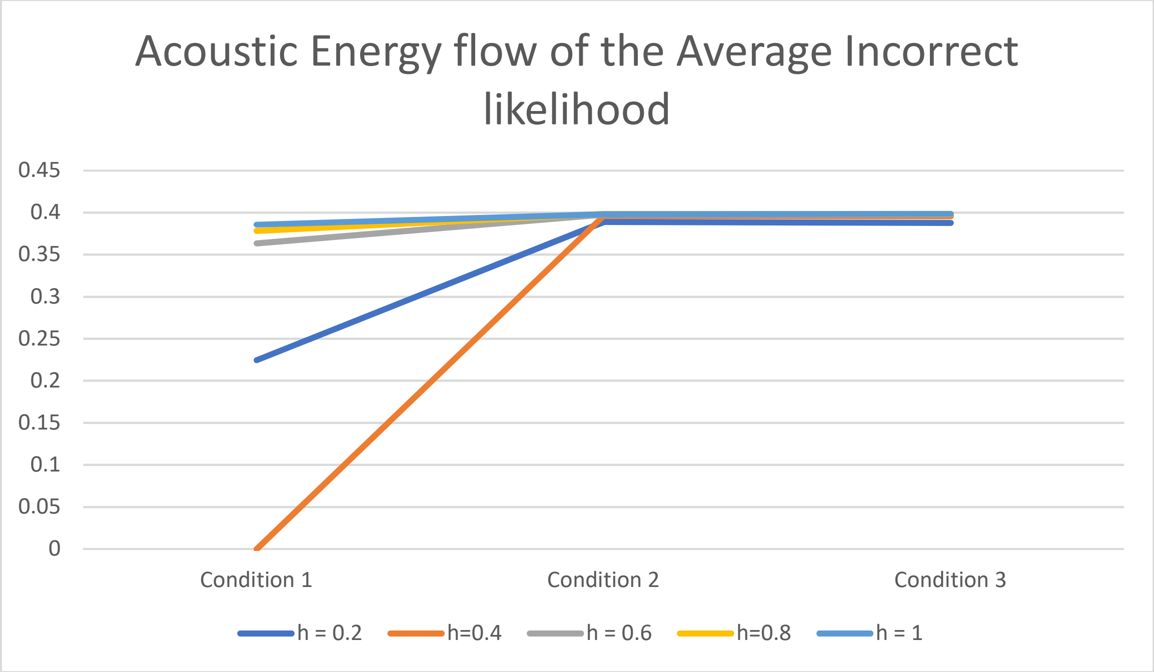

Figure 6: Acoustic Energy flow of the Average Incorrect likelihood.

IV. CONCLUSION

In this paper, the proposed Conditional Generative Adversarial Network (CGAN) is utilized in interacting cyber-physical production systems (CPPS) with IoT networking security. The conditional distributions use the CGAN model is presented to accomplish the safety of an advanced manufacturing device. The protection management issue for CPS being solved using the system dynamic feedback mechanism. CPS is configured into sub-system switching within the system. Moreover, a control strategy for recursive switching mechanism when DoS attacks are encountered based on the consistency and energy constraint of DoS attacks. The IoT-DNCS framework is enhanced to control various tasks with IoT features possible, considering participants' creation through the communication of sensors, controls, and actuators. The objective of this research brings up a variety of relevant studies in the different network-layer design, including the implementation of a more fitting SDNcontroller to handle devices and connection structures in real-time with control specifications and routing protocols. The proposed architectural model with unique integrated applications replicates its performance while evaluating the effectiveness of the proposed management system.

Acknowledgement

Funding

Not Applicable

Conflicts of interest/Competing interests

The authors declare that they have no conflict of interest. This article does not contain any studies with human participants or animals performed by any of the authors.

Availability of data and material

Not Applicable

Code availability

Not Applicable

Reference:

1. L. Monostori, "Cyber-physical production systems: Roots, expectations and r&d challenges," Procedia CIRP, 2014.
2. S. R. Chhetri et al., "Kcad: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems," in Proceedings of the 35th International Conference on Computer-Aided Design, ACM, 2016.
3. S. D. Applegate, "The Dawn of Kinetic Cyber," in 2013 5th International Conference on Cyber Conflict (CyCon), IEEE, 2013.
4. S. R. Chhetri et al., "Confidentiality breach through acoustic sidechannel in cyber-physical additive manufacturing systems." ACM Transactions on Cyber-Physical Systems, 2018.
5. S. R. Chhetri, S. Faezi, and M. A. Al Faruque, "Information leakageaware computer-aided cyber-physical manufacturing," IEEE Transactions on Information Forensics and Security, 2018.
6. D. Kushner, "The real story of stuxnet," Spectrum, IEEE, 2013.
7. R. M. Lee, M. J. Assante, and T. Conway, "German Steel Mill Cyber Attack," Industrial Control Systems, voi. 30, 2014.
8. G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies," IEEE Trans. Autom. Control, vol. 60, no. 12, pp. 3299–3304, Dec. 2015.
9. H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack policy against remote state estimation," in Proc. IEEE 52nd Annu. Conf. Decis. Control, Dec. 2013, pp. 5444–5449.
10. D. Navani, S. Jain and M. S. Nehra," The Internet of Things (IoT): A Study of Architectural Elements," 2017 13th International Conference on Signal-Image Technology and Internet-Based Systems (SITIS), Jaipur, India, 2017, pp. 473-478. doi: 10.1109/SITIS.2017.83.
11. Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, ImrichChlamtac, Internet of things: Vision, applications and research challenges, Ad Hoc Networks, Volume 10, Issue 7, 2012, Pages 1497-1516, ISSN 1570-8705.
12. Samad," Control Systems and the Internet of Things [Technical Activities]," in IEEE Control Systems, vol. 36, no. 1, pp. 13-16, Feb. 2016. doi: 10.1109/MCS.2015.2495022

13. X. M. Zhang, Q. L. Han and X. Yu," Survey on Recent Advances in Networked Control Systems," in IEEE Transactions on Industrial Informatics, vol. 12, no. 5, pp. 1740-1752, Oct. 2016. doi: 10.1109/TII.2015.2506545
14. Xiaohua Ge, Fuwen Yang, Qing-Long Han, Distributed networked control systems: A brief overview, Information Sciences, Volume 380, 20 February 2017, Pages 117-131, ISSN 0020-0255.
15. Cardenas, S. Amin, et al., "Challenges for securing cyber physical systems," in Workshop on future directions in cyber-physical systems security, 2009.
16. J. Sztipanovits. T. Bapty, S. Neema, L. Howard, and E. lackson, "OpenMETA: A model-and component-based design tool chain for cyber-physical systems," in Joint European Conferences on Theory and Practice of Software, pp. 235-248, Springer, 2014.
17. S. Markkandan, R. Logeshwaran & N. Venkateswaran (2021) Analysis of Precoder Decomposition Algorithms for MIMO System Design, IETE Journal of Research, DOI: 10.1080/03772063.2021.1920848
18. S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash," Internet of Things (IoT): A vision, architectural elements, and security issues," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 492-496. doi: 10.1109/ISMAC.2017.8058399
19. S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim and S. R. Chaudhry," IoT architecture challenges and issues: Lack of standardization," 2016 Future Technologies Conference (FTC), San Francisco, CA, 2016, pp. 731-738. doi: 10.1109/FTC.2016.7821686
20. C. l. Zhong, Z. Zhu and R. G. Huang," Study on the IOT Architecture and Access Technology," 2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), Anyang, 2017, pp. 113-116. doi: 10.1109/DCABES.2017.32
21. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017.
22. Z. Qin, G. Denker, C. Giannelli, P. Bellavista and N. Venkatasubramanian," A Software Defined Networking architecture for the Internet-ofThings," 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, 2014, pp. 1-9. doi: 10.1109/NOMS.2014.6838365
23. K. Sood, S. Yu and Y. Xiang," Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review," in IEEE Internet of Things Journal, vol. 3, no. 4, pp. 453-463, Aug. 2016. doi: 10.1109/JIOT.2015.2480421
24. N. Bizanis and F. A. Kuipers," SDN and Virtualization Solutions for the Internet of Things: A Survey," in IEEE Access, vol. 4, pp. 5591-5606, 2016. doi: 10.1109/ACCESS.2016.2607786
25. M. Ojo, D. Adami and S. Giordano," A SDN-IoT Architecture with NFV Implementation," 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, 2016, pp. 1-6. doi: 10.1109/GLOCOMW.2016.7848825
26. YustusEkoOktian, SangGon Lee, HoonJae Lee, JunHuy Lam, Distributed SDN controller system: A survey on design choice, Computer Networks, Volume 121, 2017, Pages 100-111, ISSN 1389-1286.
27. J. Wan et al.," Software-Defined Industrial Internet of Things in the Context of Industry 4.0," in IEEE Sensors Journal, vol. 16, no. 20, pp. 7373-7380, Oct.15, 2016. doi: 10.1109/JSEN.2016.2565621
28. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao," A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017. doi: 10.1109/JIOT.2017.2683200
29. J. Ren, H. Guo, C. Xu and Y. Zhang," Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," in IEEE Network, vol. 31, no. 5, pp. 96-105, 2017. doi: 10.1109/MNET.2017.1700030
30. S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," Automatica, vol. 79, no. 3, pp. 42–51, 2017.
31. Y.-C. Sun and G.-H. Yang, "Event-triggered resilient control for cyberphysical systems under asynchronous DoS attacks," Inf. Sci., vol. 465, pp. 340–352, Oct. 2018.
32. M. Wang and B. Xu, "Guaranteed cost control of cyper-physical systems under periodic DoS jamming attacks," in Proc. 37th Chin. Control Conf. (CCC), Wuhan, China, 2018, pp. 6241–6246.
33. X. Chang, R. Liu, and J. H. Park, "A further study on output feedback H∞ control for discrete-time systems," IEEE Trans. Circuits Syst. II, Exp. Briefs, to be published.
34. X. Xie, D. Yue, J. H. Park, and H. Li, "Relaxed fuzzy observer design of discrete-time nonlinear systems via two effective technical measures," IEEE Trans. Fuzzy Syst., vol. 26, no. 5, pp. 2833–2845, Oct. 2018.

35. X. Xie, Q. Zhou, D. Yue, and H. Li, "Relaxed control design of discretetime Takagi–Sugeno fuzzy systems: An event-triggered real-time scheduling approach," IEEE Trans. Syst., Man, Cybern. Syst., vol. 48, no. 12, pp. 2251–2262, Dec. 2018.
36. L. An and G. Yang, "LQ secure control for cyber-physical systems against sparse sensor and actuator attacks," IEEE Trans. Control Netw. Syst., vol. 6, no. 2, pp. 833–841, Jun. 2019.
37. L. An and G.-H. Yang, "Secure state estimation against sparse sensor attacks with adaptive switching mechanism," IEEE Trans. Autom. Control, vol. 63, no. 8, pp. 2596–2603, Aug. 2018.
38. H. Wu, W. Wang, C. Wen, and Z. Li, "Game theoretical security detection strategy for networked systems," Inf. Sci., vol. 453, pp. 346–363, Jul. 2018.
39. Y. Yuan, F. Sun, and Q. Zhu, "Resilient control in the presence of DoS attack: Switched system approach," Int. J. Control Autom. Syst., vol. 13, no. 6, pp. 1423–1435, Dec. 2015.