Taylor & Francis
Taylor & Francis Group

GAN Base feedback analysis system for industrial IOT networks

K. Ashok, Rajasekhar Boddu, Salman Ali Syed, Vijay R. Sonawane, Ravindra G. Dabhade & Pundru Chandra Shaker Reddy

Published online: 11 Nov 2022.

Submit your article to this journal ⬀

Article views: 62

View related articles ⬀

View Crossmark data ⬀

Taylor & Francis
Taylor & Francis Group

REGULAR PAPER

🔓 OPEN ACCESS | Check for updates

GAN Base feedback analysis system for industrial IOT networks

K. Ashok [a], Rajasekhar Boddu [b], Salman Ali Syed[c], Vijay R. Sonawane [d], Ravindra G. Dabhade [e] and Pundru Chandra Shaker Reddy [f]

[a]Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, India; [b]Department of Software Engineering, College of Computing and Informatics, Haramaya University, Dire Dawa, Ethiopia; [c]Department of Computer Science, Applied College, Jouf University, Tabarjal, Kingdom of Saudi Arabia; [d]Department of Information Technology, MVPS's Karmaveer Adv.Baburao Ganpatrao Thakare College of Engineering, Nashik, India; [e]Department of Electronics & Telecommunication Engineering, Matoshri College of Engineering & Research Centre, Nashik, India; [f]School of Computing and Information Technology, REVA University, Bangalore, India

ABSTRACT

The internet, like automated tools, has grown to better our daily lives. Interacting IoT products and cyber-physical systems. Generative Adversarial Network's (GANs') generator and discriminator may have different inputs, allowing feedback in supervised models. AI systems use neural networks, and adversarial networks analyse neural network feedback. Cyber-physical production systems (CPPS) herald intelligent manufacturing . CPPS may launch cross-domain attacks since the virtual and real worlds are interwoven. This project addresses enhanced Cyber-Physical System(CPS) feedback structure for Denial-of-Service (DoS) defence . Comparing sensor-controller and controller-to-actuator DoS attack channels shows a swapping system modelling solution for the CPS's complex response feedback. Because of the differential in bandwidth between the two channels and the suspects' limited energy, one person can only launch so many DoS assaults. DoS attacks are old and widespread. Create a layered switching paradigm that employs packet-based transfer techniques to prevent assaults. The discriminator's probability may be used to assess whether feedback samples came from real or fictional data. Cognitive feedback can assess GA feedback data.

1. Introduction

During the fourth industrial revolution, the German government implemented a cyber-physical manufacturing plan for small firms using artificial intelligence. It remained first made public via a workshop conducted in the US. On the other hand, a cyber system comprises elements that can compute and link to other things throughout the physical universe. The development of a fresh age within technologies used for combined cyber-physical schemes and industrial IoT nets offers statistics on a net based on a request designed for the health care businesses, bright city transport, and bright area network features. Different neural networks were combined with cognitive response methods for industrial sectors in a variety of automation device functions. According to Yann LeGunn, director of Facebook AI, generative adversarial networks (GAN) are the most intriguing machine learning concept to emerge in the previous 10 years. Generator and discriminator are the two primary elements of global adversarial networks. The generator must fetch the data before being distributed. The discriminator would calculate the likelihood that a mental response analytics system samples response data somewhat more than the original CPS and IoT data. Figure 1 depicts the IoT and Cyber-Physical System integration concept.

The fourth industrial revolution was significantly influenced by cyber-physical schemes (CPS), also recognized as cyber-physical manufacture schemes (CPPS) [1]. CPPS is a group of interconnected, cybersecurity-related subsystems connected through communication networks. Due to the intimate influences between the cyber and fleshly worlds, using CPPS would enable industrial units to become even more intelligent and dynamic. However, it may have cross-domain restrictions. Cross-domain vulnerability accomplishments include side-channel spells and then kinetic-cyber assaults [2]. Kinetic cyber-attacks remain online cyberattacks that jeopardize the trustworthiness or legitimacy of CPS [3]. Side-channel spells are efforts to take sensitive data after the digital world by detecting physical things [4,5]. All types of attacks may take advantage of other, additional slight weaknesses that target secrecy, honesty, and availability. Over 1,000 centrifuges of an Iranian nuclear reactor are physically harmed by the notorious Stuxnet worm threats [6]. In a kinetic-cyber-attack, assailants with significant explosion heater damage on a German strengthen crush [7] are included.
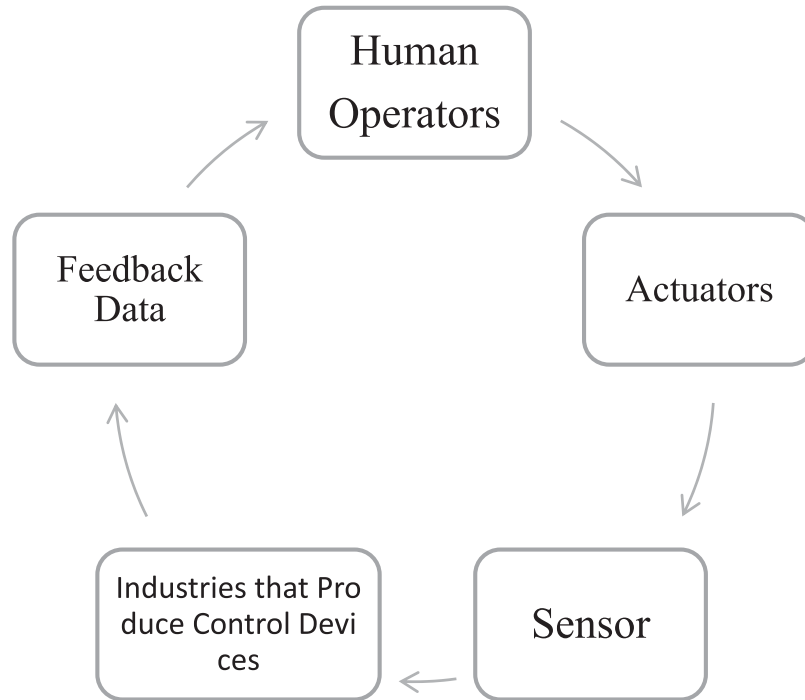

Figure 1. IoT and a cyber-physical system integrated.

Security risks, replay assaults, bogus data incursion, etc., are the current focus of the investigation into the measured protection of CPS against statement spells. Since they send a giant quantity of numbers over the network, cyber-attacks are the most hazardous and simple to execute. Because it processes this trivial information, the network cannot respond to routine service requests. By carefully constructing closed-loop poles, the system's dependability is guaranteed in the face of security attacks with erratic durations. When DoS assaults occur in a Markov process model, an ideal control technique is identified [8]. To enhance the cruel covariance drawing of the Kalman assessor from the object's viewpoint, a DoS spell outline based on a spell approach remains created in [9].

The modern Internet of Things (IoT) model introduces a distinct coating of statement and material technology that considers admission for everybody on all periods and universally and transfers mechanical arenas into an outline that practically can be related and touched in the simulated atmosphere [10]. Because of this, important device characteristics that support IoT network technology include multiplicity, optimization, universal statistics distribution via immediacy wireless knowledge, energy-optimized methods, localization and nursing skill, self-organizing landscapes, semantic interoperability, and file organization [11]. The link between control systems and IoT is very sensitive, even while the internet's closed-loop joining of fleshly objects needs fresh techniques to avoid scheme let-downs caused by incorrect material processes. Traditional feedback switch schemes assume more safely than deterministic communication.

Nevertheless, certain management-related control implementations take place online [12]. As research in various technological fields advances, challenges in control theory must be overcome. The non-deterministic schemes regulate inexpression and jitter, bandwidth, physical security, adapter devices, cyber-protection, and pattern problems [13]. Implementing Network Control Systems [14] may address several IoT challenges, including latency and jitter, but interoperability and extensibility are still problems. The common NCS solution, such as DNCS [15], expedites the transition toward the IoT age. Though, non-deterministic internet landscapes, plug-and-play tools, and interoperability may lead to unforeseen control cycles.

Due to the assumption that current spell copies might be easily functional to CPPS safety research, the attack mechanisms largely depict attackers' potential rather than the framework. Additionally, there are important research challenges while developing a recommended framework for CPS security examination: • The majority of the time, current defensive capabilities are solely advised for monitoring cyberattacks [16]. New defensive properties that may be used in the cyber-physical realms must be industrialized in instruction to lecture the research of cross-domain threats in CPPS. • The present system-level receipt perfected in CPPS aimed at the cyber-physical domain requires several Models of Computation (MoCs) [17]. • Since various subsystems connect in the CPPS environment, removing information or detecting systems must be carried out across several subsystems, which calls for a centralized device activity relevant to CPPS.

The GAN integrates the IoT environment through the present CPS background for stability and a continuing scheme.

2. Literature survey

The system's performing, control excellence, stability, and energy efficacy are all being examined using new CPPS modelling tools. These sites neglect device design's role in security. On the other hand, the bulk of the CPS's current security study concentrates on positions with known weaknesses. Without proving that the recovered device is no longer susceptible, patching programmes and deleting hardware components is advised as an ad hoc repair [18]. Eventually, a few CPS show an important character popular the CPPS, for example, a whole.

The cyber-physical system also includes viewpoints from the Internet, Semantics, and Things [19]. Sensor devices make up the experience layer. A localized communication network makes up the network layer. Finally, in the suggested structural paradigm, the presentation coating permits boundary policies to coexist through the presentation. Additionally, the middleware and gateway layers of the upgraded five-layer architecture are responsible for managing network connections and guaranteeing that the interface between the system and mesh devices is extremely flexible [20]. On the other hand, the studies' specific layer-based architectural frameworks [21,22] provide additional flexibility to meet the requirements of each application.

The quantity of available mixed interacting techniques, every by his personal traditional of admission systems and steering proprieties, increases along with the number of IoT implementations. It has been a considerable difficulty to include such components while allowing for adequate management in complicated circumstances. Several contemporary IoT design approaches [23,24] regularly depend on arranged system-based software to overcome this problem. This strategy incorporates system virtualization invention, enabling the IoT device to be adaptable and scalable [25,26]. Research has enhanced SDN-based frameworks to include a suitable controller network at the same time [27]. The fascinating applications of SDN networks for IoT are in the creative manufacturing sectors [28].

Modern edge computing approaches result from IoT systems' need for faster reaction times and higher service efficiency. The IoT tool acted like the basis meant for particular architectural ideas for an smart power system, smart transportation, and cutting-edge city projects. To identify edge technology, research on IoT elements such as infrastructure connected to the quality, stability, and privacy issues may be combined [29,30]. Even though different IoT frameworks are used for different applications, executing a method regulator organization inside closed-loop and circulated interacted regulator organizations meets a challenge that cannot be solved through the IoT background.

Stable confinement management has been proposed for irregular-time multi-agent systems through show failures [31]. Create a standard controller with the system's robustness [32] as the focal point. To protect CPS besides intermission and improver sound in the aspect of dual-channel asynchronous DoS assaults, [33] developed an innovative Event-triggered robust monitoring approach. Two distinct event-triggering methods have been created for both S–C and C–A channels. State-input control is used when transmission dropouts brought on by DoS assaults are encountered [34].

On the other hand, the method's condition may not always be quantified. A lively exterior view regulator in a connected productivity reaction regulator is used to determine the condition of the regulated device. Investigated are H challenges [35]. Depending on the case cause function, nonlinear observer-dependent output feedback control. Several problems still need to be resolved, even though admission checking difficulties besides DoS assaults investigated popular the non-fiction [36,37]. The most challenging issue is properly explaining how systematic assaults affect functioning. Attack limit and strength are chosen to show how attackers and machine effectiveness interact. A two-stage optimization method is used to study the formal requirements of Nash equilibrium.

Although the scheme essential takes an optimal calculation bound depending scheduled danger amount in the face of intellectual threats, it may successfully minimize transmission dropouts by DoS assaults. Investigate the systematic switching method for dynamic monitoring and propose a mixture scientific model wherever the manager shifts based scheduled the conflicting outcomes of the cyber attacker and the defense. Furthermore, the categorization method does not take into account the impact of DoS assaults that are systematic and target different contact networks. By categorizing substituting subsystems built scheduled the characteristics of determined DoS assaults, it will be possible to handle the problem of DoS spells aimed at virtual-fleshly organizations and then avoid the duration of DoS spells. Typically, the controller uses a sequence of anticipated coming controller participations to optimize the Cyber-Physical System during Denial-of-Service assaults.

3. System model

The Generative Adversarial Networks (GAN) that have been proposed container stand cast-off in various

modern submissions with various structural frameworks, including the generation of image features using Convolutional Neural Networks, variant data types with fully connected networks, and sequence data type recurrent network models. Figure 2 depicts the GAN model's layout. The suggested algorithmic technique examines contribution statistics through accomplishing the fast development that consumes highlighted synthetic intellect. Particularly, conditional GANs and unconditional GANs are two categories for systematic models. The GAN model's generator and discriminator are affected, which helps verify the input data. A few current uses of generative adversarial networks include semi-administered calculating, picture removal, copy capture, response statistics gathering, software optimization, and calculating (GAN).

A typical Cyber-Physical Protection System (CPPS) configuration comprises several subsystems.

Signal and energy fluxes, which may exist inside subsystems, connect the constituents in each subsystem's cyber and physical realms. The suggested paradigm facilitates interaction between the various flows across several subsystems or within a single subsystem. The Conditional Generative Adversarial Model may achieve this (CGAN). The amount of time needed to be aimed at sign and liveliness currents is calculated during the CPPS enterprise phase dependent on the special device design. Different nodes are used to achieve the cyber and physical realms, while edges are used to move energy and signals across various nodes. To represent every potential flow and allow us to determine the flow pairings, the distinctive pattern in the designed CPPS is used. Every unique pair for the suggested model is generated using the CGAN. Deduce the highest level of a probability distribution using the information about each flow, allowing for a tight relationship between the two flows. The distribution and interaction among many currents are improved after a safety viewpoint. The suggested CGAN organized classical provides an academic foundation aimed at the development then analysis of CPPS that combats irritated-field intimidations on the scheme equal, depending on the security strategy. An integrated IoT network facility improves CGAN-founded safety aimed at the Virtual-Fleshly Safety Scheme (CPPS).

With a tool for CPPS, the suggested CGAN system model generates and resolves security analyses in two steps. The two steps of the suggested system model are Graph Construction and CGAN-based Security. The design time and the informative data from the subsystems in CPPS are inputs used by the network development algorithm. To improve the visual representation from the existing CPPS, each subsystem's virtual and fleshly world components remain assessed to match the drive and sign current statistics inside a subsystem.

Procedure for Safety study:

Discriminator, producer, sound below complaint, incidence article directories, and Parzen Gap by Breadth "h" are all inputs.

Production: Probability Metrics: AvgCorLike stands for regular, precise probability, and AvgLncLike for regular improper probability.

Step 1: Create a matrix with the dimensions batch size (N) x step size and initialize AvgCorLike and AvglncLike (K).

Step 2: Right Probability (CorLike)0, precise amount (CorNum), improper probability (IncLike), and improper amount (IncNum) remain initialized toward nothing when the random condition falls within the given state.

Step 3: To begin, samples XGwith G(Z|Condi) for each condition mark Condi are produced.

Step 4: Aimed at an assumed Parzen gap scope h then present function directory Ftldx, we generate a provisional approximation delivery FtDistr $= \Pr(XGFTIdx|$ Condi) using the Parzen Gaussian Window method.

Step 5: Founded happening the likelihood aimed at all examples usual. We update two parameters and construct the appropriate examination examples for all incidence purposes inside the examination pack Xtest.

Step 6: Founded the number of examination examples for each purpose. The aggregate of CorLike and IncLike is then determined.

Step 7: Depending on the circumstances, binary circles of regular metrics, AvgCorLike then AvglncLikeare, are changed by the comparable sets of combined measured data.

The internet has expanded to benefit our everyday life in the current technological era, including automation gadgets, for new industries, cyber-physical CPSs, and industrial Internet of Things (IoT) devices. GANs, for example, might be used to provide perceptual assessments in a supervised learning model using separate data for the generator and discriminator. Adversarial networks, as opposed to neural networks in artificial intelligence systems, use data to analyse feedback analytics. When cyber-physical production technologies are adopted, a new age of intelligent manufacturing will begin CPPS. CPPS, on the other hand, is susceptible to cross-domain assaults because to the linkages among the simulated and natural worlds. This work aims to provide enhanced performance feedback management for CPSs in order to mitigate Denial-of-Service DoS attacks CPS. A exchanging system modelling methodology for the complicated reaction reply, CPS, is shown by evaluating the different impacts of DoS attacks on the sensor-controller S–C and controller-to-actuator C-A channels. Because of the bandwidth differential concerning the double networks as well as the defendant's drive limitations, he remains acceptable to suppose that a delinquent be able to only jam one transmission stream at a time.
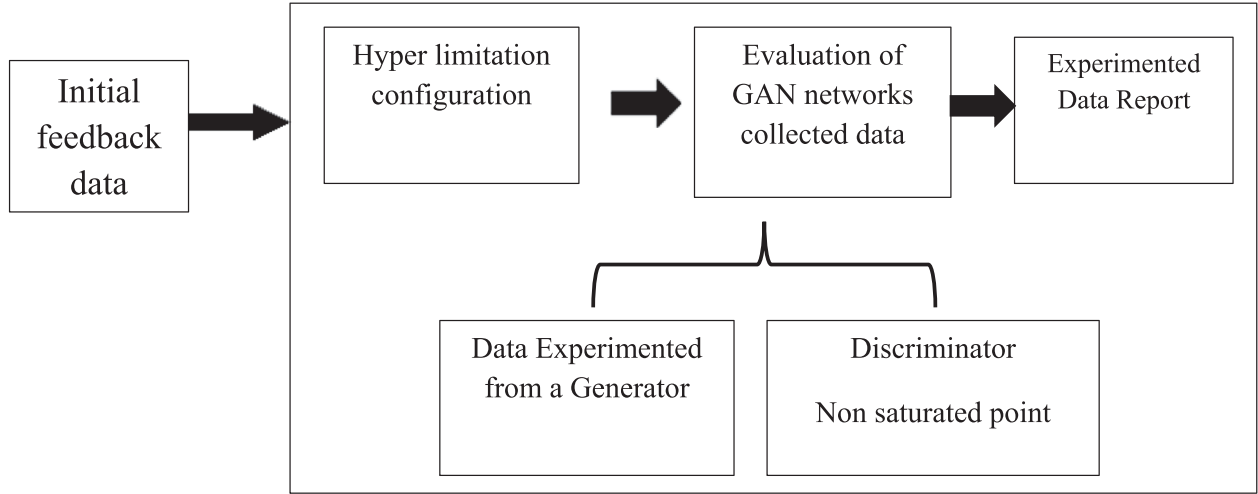
Figure 2. Design of generative adversarial networks.

Layered switching is then built, considering geographic variety and the historical durability of DoS attacks. To evaluate if samples were chosen from legitimate or fraudulent data, feedback data is examined using the discriminator's probability. Cognitive feedback assists genetic algorithms for cutting-edge technology in analysing feedback data. The internet has expanded to benefit our everyday life in the current technological era, including automation gadgets, for new industries, CPSs, and industrial Internet of Things IoT strategies. GANs, for example, might be used to provide perceptual assessments in a supervised learning model using separate data for the generator and discriminator. Adversarial networks, as opposed to neural networks in artificial intelligence systems, use data to analyse feedback analytics. When cyber-physical production technologies are adopted, a new age of intelligent manufacturing will begin CPPS. To evaluate if samples were chosen from legitimate or fraudulent data, feedback data is examined using the discriminator's probability. Cognitive feedback assists genetic algorithms for cutting-edge technology in analysing feedback data.

The CPS is scrambled along together with a worth of $\varepsilon_{I,n} > 1, \mu > 1$ indicates that it is exponentially steady each the delay ratio of $^{2(N+2)}\sqrt{\rho}$. The highest successive rises expected to DoS spells is offered in conditions of $P_{I,n} > 0 (i \in M, n \in L)$, in which the limited collection is designated as L.

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

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

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

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

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,

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

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

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

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

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

The most appropriate Lyapunov function for the system is selected.

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

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

$$\Delta W_{i,n}(k_t) = W_{i,n}(k_{t+1}) - W_{i,n}(k_t)$$
$$\Delta W_{i,n}(k_t) = \xi^T(k_t)\Omega_{i,n}\xi(k_t) \quad (9)$$

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 $W_{i,n}(k_t) < W_{i,n}(k_0)$.

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

The performance of Schur completes the lemma through $\Omega_{I,n} < 0$ the equal disparity matrix is found.

$$V_{\tau\sigma(k_t)^{(k_t)}}(k_{t+1}) = z^T(k_{t+1})P_{\tau\sigma(k_t)^{(k_t)}}z(k_t) \quad (11)$$

The transmission switching point is used to find the equivalent smallest packet transmission point at $N(N+1)$ time steps. As a result, given the delay rate, the cyber-physical system CPSs is exponentially steady at limited instant increments.
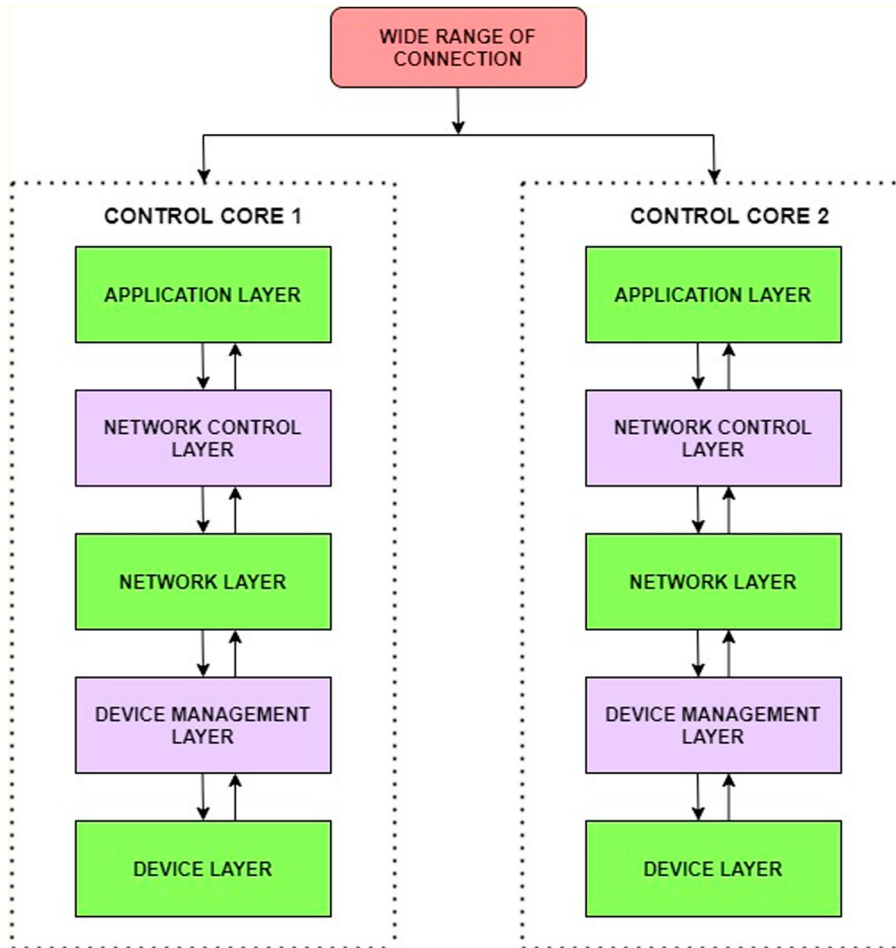
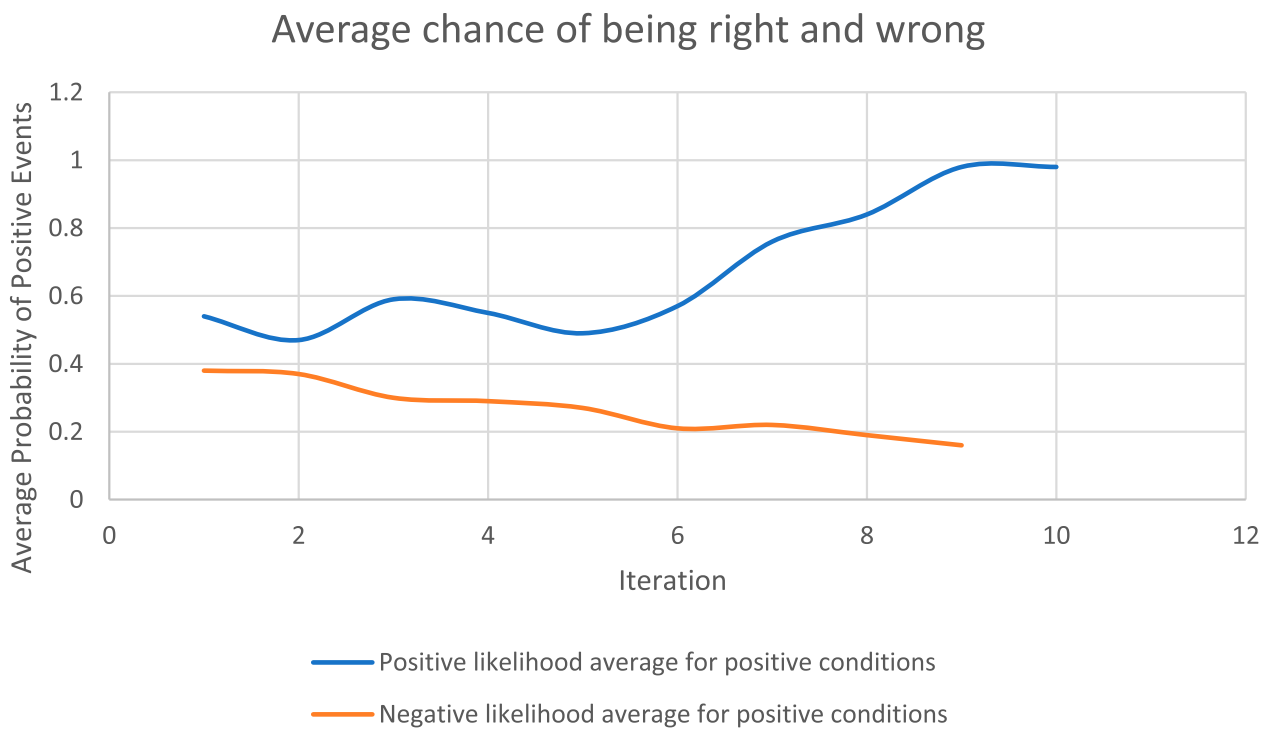**Figure 3.** IoT-founded dispersed net switch scheme.

Figure 4. Typical odds of being right and wrong for iterations with h = 0.2.
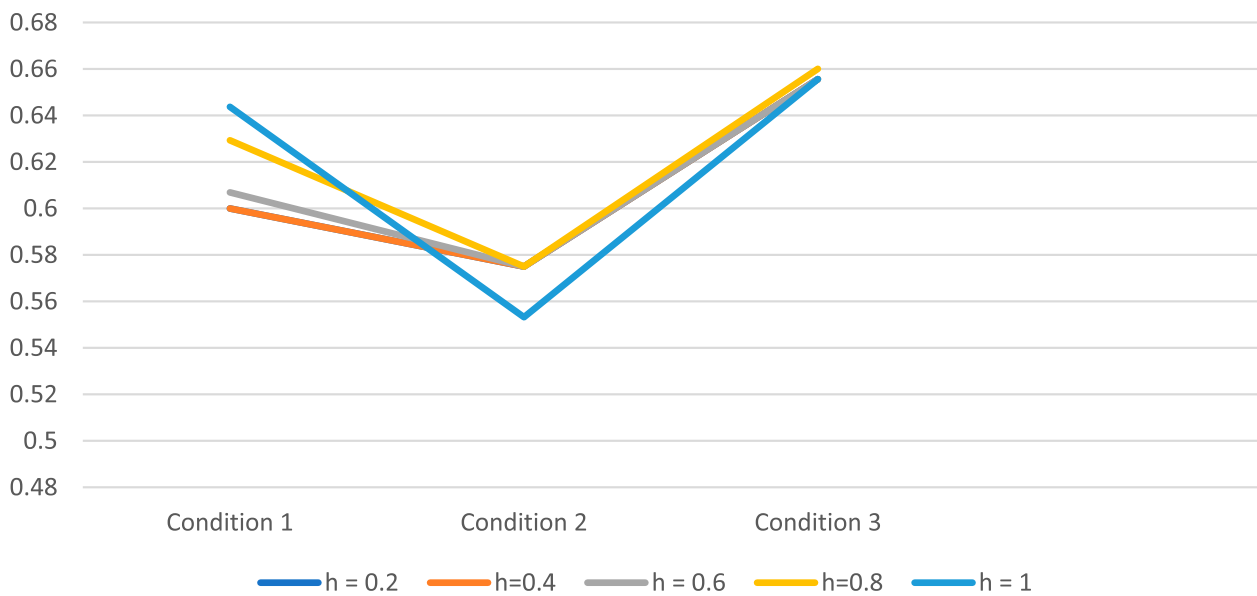
Average accurate probability acoustic energy flow

Figure 5. The accurate average probability of the acoustic energy flow

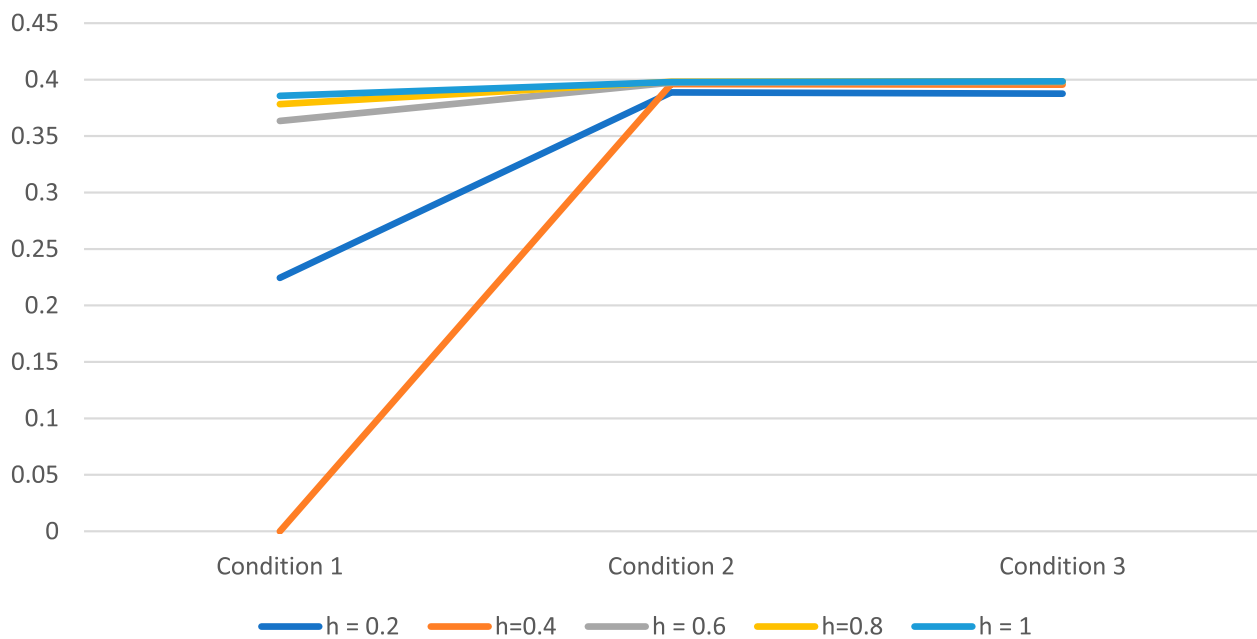## Average Incorrect Likelihood Acoustic Energy Flow

Figure 6. Average incorrect likelihood acoustic energy flow.

4. Result and discussion

To fully meet the DNCS requirement, a layer-based structure is constructed while considering IoT technical improvements. Figure 3 displays an IoT-based distribution network concept. IoT DNCS is represented by the control core. The control core serves as the foundation for communication between the five prepared layers: application, network control, network, management, and device. The management tools used by the investigators to control system functionality are

likewise located in the interface layer. Sensors, actuators, and controllers are all utilized in the proposed system paradigm. Unidentified data volumes inside the layer are understood to have plug-and-play capability that remains determined on before autonomous of spell. When comments remain wanted, devices remain positioned to capture the necessary material, and lively organizers monitor the switch signs. Uncertainty the construction of an entity is required, the received actuators utilize control signals to provide protection. The three responsibilities involved in device governance are

the primary goals of the system organization flat in terms of the scheme coating. The sensors first check the data incoming then departing the scheme, then evaluate the device's efficiency then ability toward do controls aimed at the researcher's progress, and then decide founded happening a specified usual of criteria. The actuators are managed in the second step by identifying the data entering and leaving a scheme, measuring the actuator's convenience then capacity to count measured signs aimed at detective formation, then determining whether bury-supervisor swapping is practically based on net switch conditions. The third stage remains toward manage the actuators, which includes measuring incoming then outgoing statistics from a scheme, calculating the amount of operative groundwork required, then changing the actuators in accordance with the contact network and member control standards.

The network layer oversees collecting statistics after the south-bound coating then communicating it across connection-oriented nets. This network's hub has the hardware and networking technologies necessary to connect to a variety of enterprises. This layer also handles route identification for a steady connection, which improves message among switch centres. The Net Switch Coating remains the greatest crucial meanwhile he allows DNCS toward purpose efficiently cutting-edge an IoT environment. The capabilities of the interacting perfect are achieved through sending the net coating to the tool organization coating. The net switch coating may intellectual work-related organization nets autonomously through authorizing IoT procedure connections by diverse devices in terms of connectivity and understanding exchange that may enter then depart the scheme on different times. The net switch coating determines when the expedient coating makes contribution statistics, interacts with net coating components, then when sensors, actuators, and controllers are activated (Figure 4).

The easiest way to determine if there is Z-motor movement in the G/M-code is to consider an invasive situation, symbolized by the motor moving in either the X or Y direction, as illustrated in Figures 5 and 6. The user could also foresee the results of any integrity and accessibility attack prediction model necessary to recognize side-channel assaults on certain X, Y, or Z motor components using the suggested CGAN typical.

5. Conclusion

It is used in this research to examine the security of IoT networking and CPPS with the proposed CGAN. To assure the safety of a gadget during advanced manufacturing, we use conditional distributions based on the CGAN model. The CPS protection management issue is being addressed via the system dynamic feedback mechanism. Switching between subsystems is done via

CPS. The frequency of Denial-of-Service (DoS) attacks and energy limits may also be used to govern recursive switching processes. We've reworked the IoT-DNCS framework to use the growing number of sensors, controllers, and actuators available via the Internet of Things. There are several practical applications for this topic, such as strengthening the SDN controller's ability to operate methods then joining topologies in actual via switch requirements then direction-finding procedures. Special integrated apps are used in the proposed architectural paradigm to assess the management system's effectiveness while simulating its performance.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

K. Ashok http://orcid.org/0000-0003-2329-9634
Rajasekhar Boddu http://orcid.org/0000-0002-2522-206X
Vijay R. Sonawane http://orcid.org/0000-0002-1998-0622
Ravindra G. Dabhade http://orcid.org/0000-0002-7659-1850
Pundru Chandra Shaker Reddy http://orcid.org/0000-0002-3643-0753

References

[1] Monostori L. Cyber-physical production systems: roots, expectations and r&d challenges. Procedia CIRP. 2014; 17:9–13.
[2] Chhetri SR, Canedo A, Al Faruque MA, et al. KCAD: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems. Proceedings of the 35th International Conference on Computer-Aided Design; 2016; ACM.
[3] AlZubi AA, Al-Maitah M, Alarifi A. Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Comput. 2021;25: 12319–12332. doi:10.1007/s00500-021-05926-8.
[4] Ponnan S, Saravanan AK, Iwendi C, et al. An artificial intelligence-based quorum system for the improvement of the lifespan of sensor networks. IEEE Sensors J. 2021;21(15):17373–17385.
[5] Kushner D. The real story of stuxnet. IEEE Spectrum. 2013;50(3).
[6] Lee RM, Assante MJ, Conway T. German steel mill cyber attack. Ind Control Syst. 2014;30:62.
[7] Befekadu GK, Gupta V, Antsaklis PJ. Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies. IEEE Trans Autom Control. 2015 Dec;60(12):3299–3304.
[8] Zhang H, Cheng P, Shi L, et al. Optimal DoS attack policy against remote state estimation. Proceedings of the IEEE 52nd Annual Conference on Decision and Control; 2013 Dec. p. 5444–5449.
[9] Navani D, Jain S, Nehra MS. The internet of things (IoT): A study of architectural elements. 2017 13th International Conference on Signal-Image Technology and Internet-Based Systems (SITIS); 2017; Jaipur, India. p. 473–478. doi:10.1109/SITIS.2017.83.

[10] Miorandi D, Sicari S, De Pellegrini F, et al. Internet of things: vision, applications and research challenges. Ad Hoc Netw. 2012;10(7):1497–1516. ISSN 1570-8705.

[11] Samad T. Control systems and the internet of things [technical activities]. IEEE Control Syst. 2016 Feb;36(1):13–16. doi:10.1109/MCS.2015.2495022.

[12] Zhang XM, Han QL, Yu X. Survey on recent advances in networked control systems. IEEE Trans Ind Inf. 2016 Oct;12(5):1740–1752. doi:10.1109/TII.2015.2506545.

[13] Ge X, Yang F, Han Q-L. Distributed networked control systems: a brief overview. Inf Sci. 2017 Feb 20;380:117–131, ISSN 0020-0255.

[14] Cardenas S, Amin S, Sinopoli B, et al. Challenges for securing cyber physical systems. Workshop on Future Directions in Cyber-physical Systems Security; 2009.

[15] Sztipanovits J, Bapty T, Neema S, et al. OpenMETA: A model-and component-based design tool chain for cyber-physical systems. Joint European Conferences on Theory and Practice of Software; 2014; Springer. p. 235–248.

[16] Markkandan S, Logeshwaran R, Venkateswaran N. Analysis of precoder decomposition algorithms for MIMO system design. IETE J Res. 2021:1–8.

[17] Vashi S, Ram J, Modi J, et al. 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); 2017; Palladam. p. 492–496. doi:10.1109/ISMAC.2017.8058399.

[18] Al-Qaseemi SA, Almulhim HA, Almulhim MF, et al. Iot architecture challenges and issues: lack of standardization. 2016 future Technologies Conference (FTC); 2016; San Francisco, CA. p. 731–738. doi:10.1109/FTC.2016.7821686.

[19] Zhong Cl, Zhu Z, Huang RG. Study on the IOT architecture and access technology. 2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES); 2017; Anyang. p. 113–1116. doi:10.1109/DCABES.2017.32.

[20] Sethi P, Sarangi SR. Internet of things: architectures, protocols, and applications. J Electr Comput Eng. 2017;2017:1–25. 25 pages. Article ID 9324035.

[21] Qin Z, Denker G, Giannelli C, et al. A software defined networking architecture for the internet-ofThings. 2014 IEEE Network Operations and Management Symposium (NOMS); 2014; Krakow. p. 1–9. doi:10.1109/NOMS.2014.6838365.

[22] Sood K, Yu S, Xiang Y. Software-defined wireless networking opportunities and challenges for internet-of-things: a review. IEEE Internet Things J. 2016 Aug;3(4):453–463. doi:10.1109/JIOT.2015.2480421.

[23] Bizanis N, Kuipers FA. SDN and virtualization solutions for the internet of things: a survey. IEEE Access. 2016;4:5591–5606. doi:10.1109/ACCESS.2016.2607786.

[24] Ojo M, Adami D, Giordano S. A SDN-IoT architecture with NFV implementation). 2016 IEEE Globecom Workshops (GC Wkshps); 2016; Washington, DC. p. 1–6. doi:10.1109/GLOCOMW.2016.7848825.

[25] Oktian YE, Lee SG, Lee HJ, et al. Distributed SDN controller system: A survey on design choice. Comput Netw. 2017;121:100–111. ISSN 1389-1286.

[26] Wan J, et al. Software-Defined industrial internet of things in the context of industry 4.0. IEEE Sensors J. 2016 Oct 15;16(20):7373–7380. doi:10.1109/JSEN.2016.2565621.

[27] Lin J, Yu W, Zhang N, et al. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. 2017 Oct;4(5):1125–1142. doi:10.1109/JIOT.2017.2683200.

[28] Ren J, Guo H, Xu C, et al. Serving at the edge: a scalable IoT architecture based on transparent computing. IEEE Network. 2017;31(5):96–105. doi:10.1109/MNET.2017.1700030.

[29] Feng S, Tesi P. Resilient control under denial-of-service: robust design. Automatica (Oxf). 2017;79(3):42–51.

[30] Sun Y-C, Yang G-H. Event-triggered resilient control for cyberphysical systems under asynchronous DoS attacks. Inf Sci. 2018 Oct;465:340–352.

[31] Wang M, Xu B. Guaranteed cost control of cyperphysical systems under periodic DoS jamming attacks. Proceedings of 37th Chinese Control Conference (CCC); 2018; Wuhan, China. p. 6241–6246.

[32] Chang X, Liu R, Park JH. A further study on output feedback H∞ control for discrete-time systems. IEEE Trans Circuits Syst II, Exp Briefs; 67(2):305–309.

[33] Xie X, Yue D, Park JH, et al. Relaxed fuzzy observer design of discrete-time nonlinear systems via two effective technical measures. IEEE Trans Fuzzy Syst Oct. 2018;26(5):2833–2845.

[34] Leonid TT, Jayaparvathy R. Retracted article: statistical–model based voice activity identification for human-elephant conflict mitigation. J Ambient Intell Human Comput. 2021;12:5269–5275.

[35] An L, Yang G-H. Secure state estimation against sparse sensor attacks with adaptive switching mechanism. IEEE Trans Autom Control. 2018 Aug;63(8):2596–2603.

[36] Wu H, Wang W, Wen C, et al. Game theoretical security detection strategy for networked systems. Inf Sci Jul. 2018;453:346–363.

[37] Yuan Y, Sun F, Zhu Q. Resilient control in the presence of DoS attack: switched system approach. Int J Control Autom Syst. 2015 Dec;13(6):1423–1435.