

# An In-Depth Examination of Artificial Intelligence-Enhanced Cybersecurity in Robotics, Autonomous Systems, and Critical Infrastructures

Fendy Santoso, *Senior Member, IEEE* and Anthony Finn

**Abstract**—Recent developments in cutting-edge robotics have been constantly faced with increased cyber-threats, not only in terms of the quantity or the frequency of attacks, but also when it comes to the quality and the severity of the intrusions. This paper provides a systematic overview and critical assessment of state-of-the-art scientific developments in the security aspects of robotics, autonomous systems, and critical infrastructures. Our review highlights open research questions addressing significant research gaps and/or new conceptual frameworks, considering recent advancements in artificial intelligence (AI) and machine learning. Thus the contributions of this paper can be summarised as follows. We first compare and contrast the benefits of multiple cutting-edge AI-based learning algorithms (e.g., fuzzy logic and neural networks) relative to traditional model-based systems (e.g. distributed control and filtering). Subsequently, we point out some specific benefits of AI algorithms to quickly learn and adapt the dynamics of non-linear systems in the absence of complex mathematical models. We also present some potential future research directions (open challenges) in the field. Lastly, this review also delivers an open message to encourage collaborations among experts from multiple disciplines. The implementation of multiple AI algorithms to tackle current security issues in robotics will transform and create novel, hybrid knowledge for intelligent cybersecurity at the application level.

**Index Terms**—Cybersecurity, Artificial Intelligence, Machine Learning, robotics, autonomous systems, and critical infrastructures.

## I. INTRODUCTION

Robotics and autonomous systems are complex networked system, comprising of computers, software or algorithms, and physical entities (e.g. sensors and actuators), connected in feedback mechanisms to achieve its intelligent purpose. There are myriad examples of modern robots and autonomous systems in society, starting from autonomous

Fendy Santoso is with the Artificial Intelligence and Cyber Futures (AICF) Institute, Charles Sturt University, Bathurst, NSW 2795, Australia. He was also with the Defence and Systems Institute, UniSA STEM (Science, Technology, Engineering, and Mathematics), The University of South Australia, Mawson Lakes, SA 5095, Australia.

Anthony Finn is with the Defence and Systems Institute, UniSA STEM (Science, Technology, Engineering, and Mathematics), The University of South Australia, Mawson Lakes, SA 5095, Australia.

Corresponding Author: Fendy Santoso, Email: fendy\_santoso@yahoo.co.uk.

This research was supported by The United States Army Futures Command (AFC), The United States Army Combat Capabilities Development Command (DEVCOM) - Ground Vehicle Systems Center (GVSC), and The International Technology Center Indo-Pacific (ITC-PAC) under contract FA5209-18-P-0146 ITC PAC Fund for “Trusted Operations for Robotic Vehicles in Contested Environments.”

vehicles [1,2], automatic process control [3], as well as industrial and flight control systems [4]. Thus, it is apparent that the intellectual challenge of research in this area is highly multidisciplinary as it covers a spectrum of scientific disciplines.

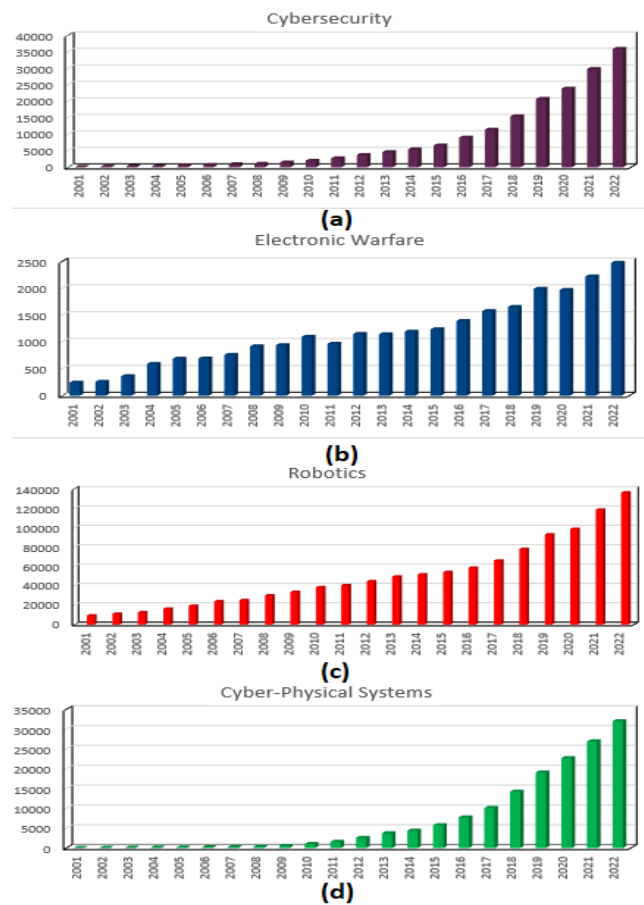


Fig. 1. Scopus data, depicting current trend of particular research themes, namely, (a) cybersecurity, (b) Electronic Warfare, (c) Robotics (d) Cyber-Physical System from 2001-2023. While the vertical axis depicts the number of publications in a particular year, the horizontal axis points out the historical time-line of our interest.

According to the data obtained from the SCOPUS publication database (see Fig. 1), the annual rate of publicly available, peer-reviewed archival manuscripts in the area of cybersecurity has increased exponentially from around 140 papers in 2001 to more than 24,000 papers in 2021. By comparison, the publicly available publication rate for the field of electronic warfare has

increased from about 250 papers in 2001 to more than 1800 papers in 2021. Similarly, the number of papers in robotics has skyrocketed over the same period. To some extent, this growth has likely been driven by the advent of the newly established research field of cyber-physical systems, which has rapidly increased to more than 15,000 publications in 2019 from almost nothing in 2001. In fact, publications in this area have increased substantially from 16,000 papers in 2019 to about 23,000 manuscripts in 2021.

From Fig. 1, one can also easily conclude that, in terms of relative popularity, research in the area of cyber-physical systems (including security aspects in robotics and autonomous systems) still has room to expand. This is indicated by a steady annual publication rate in recent years, despite the inter-disciplinary nature and large coverage of this field of study. The SCOPUS statistical data also suggest that researchers still heavily focus on the general performance and innovations of robots rather than investigating the potential cyber-threats at the application levels.

Intertwined with its functionality and performance, another important aspect worth considering when designing an autonomous system is security and privacy as cybersecurity has become everyone's business. For instance, a robotic cyberattack has posed a very serious threat to society. The scope of the attacks are varied and typically range from computational resources [5], communication links [6], operating systems [7] as well as software libraries, sensor data, and information fusion [8].

While having similar objectives (i.e. to target the vulnerability of sensors and communication links), cyberattack slightly differs from electronic warfare, which mainly relies on the use of electromagnetic spectrum to attack, assault, or impede the enemy (i.e. spoofing [9], jamming [10], and blinding [11]). While the latter generally manipulates signals through sensory inputs (a GPS or radar as in [9]), cyberattacks focus on falsifying sensory data.

A cyberattack may therefore exploit vulnerabilities of a robot's operating systems (O/S), such as Windows and Ubuntu (Linux), or its middleware, such as ROS (Robot Operating System), which can be thought of as a set of software libraries that bridge the robot's O/S and its applications or database; both of which are very susceptible to any intrusions [12].

The prediction that the speed of computers doubles every two years (Moore's law) has paved the way for the development of new theories and applications in AI. In fact, current advancements in AI have radically changed many aspects of robotics and automation. For instance, in the area of robotic control, AI has led to the birth of numerous intelligent guidance and control methods. Many model-free, intelligent guidance and control approaches have been introduced, such as fuzzy systems [13], missile guidance based on robust predictive control using neural-network optimization [14], hybrid neuro-fuzzy control systems [15], and genetic algorithms [16] to name a few. When it comes to computer vision and other sensory systems, AI and machine learning algorithms have been also implemented to perform accurate tracking [17], bio-inspired computing of vision [18] and pattern recognition [19].

In the area of cybersecurity, likewise, many researchers

have leveraged the benefits of AI to predict certain anomalies. For instance, [20] and [21] employed fuzzy systems for an embedded network of security cyber sensors, [22] discussed the application of neural networks in cybersecurity, and [23] used genetic algorithms to improve network security.

With all these cutting-edge developments, the key research questions are:

- 1) To what extent have AI revolutionized the field of cyber-physical systems, connecting dots between robotic cyberattacks and machine learning?
- 2) How much impact has AI had in the field of cybersecurity in robotics and autonomous systems?
- 3) What are potential research avenues for both theoretical and practical aspects of robotics cybersecurity?

Answering the above research challenges, our review paper aims to complement the existing review papers, whose focus are different, namely, [24] investigating the general security issues at the various layers of communication; [25] and [26], focusing on the interconnection of robotics and the Internet-of-Things Systems as well as [27] discussing secure estimation and control for autonomous power systems.

Hence, the main unique contributions of our paper are to provide an overview of the state-of-the-art cybersecurity systems, connecting dots between robotics, autonomous systems, critical infrastructures, and cutting-edge machine learning algorithms as follows:

- 1) We first discuss the motivations behind this research theme and the importance of cybersecurity in various areas of robotics and automation while highlighting the pros and cons of the existing algorithms.
- 2) We highlight some potential security issues, associated with the most widely implemented middleware software in robotics, namely, the Robot Operating Systems (ROS).
- 3) We discuss the pros and cons of several cutting-edge algorithms, widely implemented in such systems, especially when it comes to the roles of multiple AI algorithms, i.e. type-1 and type-2 fuzzy systems, neural networks, genetic algorithms, as well as machine learning (deep learning) algorithms and some hybrid approaches that turn out to be quite effective. This also includes some potential limitations of the existing techniques and how to improve the performance of the system.
- 4) Finally, we speculate about some potential future directions in this area.

The paper is structured as follows. Section II describes the general problem statement of cybersecurity in autonomous systems. Section III presents an overview of the most widely implemented middleware in robotics, namely, the Robot Operating System (ROS). This section highlights the pros and cons of ROS a middleware platform widely used in robotics. Meanwhile, Section IV discusses cybersecurity at the application layer, leveraging the benefits of several cutting-edge AI and machine learning algorithms, eliminating the requirements to dig deeper into the middleware of the source code to detect faults. Those algorithms serve as powerful tools to solve

the our problem statement presented in Section II. Moreover, Section V discusses some potential research challenges while summarising the benefits of some cutting-edge AI algorithms. Section VI concludes this paper and speculates some potential future research directions for the field.

## II. MATHEMATICAL PROBLEM FORMULATION

To formulate the problem, as a working example, we employ a typical feedback control system widely implemented in cyber-physical systems.

It is understood that security can be compromised at multiple different levels within the UAV, e.g. at the system, sub-system, component, or sub-component levels. For instance, when it comes to a sensory system such as a LIDAR (Light Detection and Ranging) or a camera, this may be attacked at the signal processing (distance measurement) level or the sensor fusion (application) level.

Given the nonlinear dynamics of autonomous systems with feedback control for  $N$  sub-systems, the (i,j)-th components can be represented using the following non-linear state space equation:

$$\begin{cases} \dot{x}_{i,j}(t) = f_{i,j}(x_{i,j}(t)) + g_{i,j}(x_{i,j}(t))u_i(t) \\ + \delta_{i,j}(y(t)) + d_{i,j}(t), \forall t \geq 0, \\ y_i(t) = x_{i,j}(t) + \delta_o(t), \quad i = 1, 2, \dots, N, \quad j = 1, 2, \dots, M - 1 \end{cases} \quad (1)$$

where  $x_{i,j} \in \mathbb{R}^j$  is the state vector of the system, whose values are bounded within its maximum and minimum range,  $\underline{x}_{i,j} \leq x_{i,j} \leq \bar{x}_{i,j}$ .  $\underline{x}_{i,j}$  may be corrupted by  $\delta_{i,j}$ , a vector of malicious attacks on a particular system state, where  $(u_i, y_i) \in \mathbb{R}$  denote the control inputs and system outputs, bounded such that  $\underline{u}_i(t) \leq u_i(t) \leq \bar{u}_i(t)$  and  $\underline{y}(t) \leq y(t) \leq \bar{y}(t)$  that denotes the vector of system output, and which may be corrupted by  $\delta_o(t)$ , a vector of malicious attack attempting to spoof the output of the system. Meanwhile  $f_{i,j}(\cdot)$  and  $g_{i,j}(\cdot)$  indicate the unknown smooth functions describing the non-linear dynamics of the systems while  $d_{i,j}$  presents the external disturbance on the system states.

The following performance index  $J$  in (2) will have feasible and finite solutions, making it possible to estimate the system state  $\forall t \geq 0$  to verify the truthfulness of the states, i.e.

$$\arg \min J = \arg \min \|y(\cdot) - \hat{y}(\cdot)\|_2, \forall t \geq 0, \quad (2)$$

where  $y(\cdot)$  denotes the actual output of the system,  $\hat{y}(\cdot)$  is the predicted output of the system, and  $\|\cdot\|_2$  is the Euclidean norm. Equation (2) clearly indicates that for the case of legitimate users, given a stable state estimator, the predicted values will converge to zero, such that the tracking error is  $e = \|y(\cdot) - \hat{y}(\cdot)\|_2 \rightarrow 0$ . On the other hand, if the real state values are compromised, the condition in (2) may not be satisfied (e.g. due to malicious data injections), and accordingly the tracking error shall not converge.

## III. OVERVIEW OF ROBOT OPERATING SYSTEMS: ROS, SROS, ROS2.0, AND ROS-M ARCHITECTURE

In this section, we discuss the cyber vulnerability of ROS, a widely implemented middleware containing a communications

platform and repository of libraries that form a bridge between a robot's operating system (O/S) and its applications. It is important since the operating system plays an essential role (the core of any software) in managing all of the computational processes, memory, data transfer, communications, and networking. Without a powerful O/S, a computer is essentially useless.

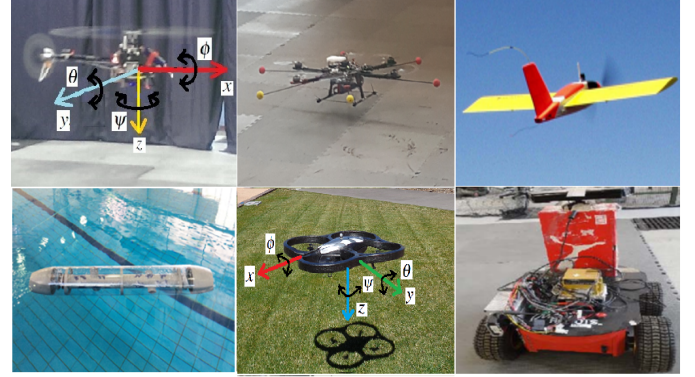


Fig. 2. Relying on ROS platform, various unmanned vehicle platforms are vulnerable to cyber-threats, starting from (a) Top Left: an unmanned helicopter [28], (b) Top middle: a hexacopter rotorcraft [29], (c) Top right: the P15035 flying wing aircraft due to Monash Aerobotics Research Group [30], (d) Bottom left: an underwater vehicle [31], (e) Bottom Middle: the AR.Drone quadcopter rotorcraft [32], and (f) Bottom Right: the Pioneer 3-AT ground robot [33].

Originally designed by Willow Garage in 2007 for use with the PR2 robot [34], a single humanoid robot for research applications in academia, ROS provides an open, modular and flexible architecture for autonomous systems. Due to the many advantages of ROS, the system has gained popularity. As a result, its adoption has gone well beyond the academic research community and it has been used in a variety of areas, e.g. agriculture [35] and home robots [36]. NASA is even expected to employ ROS on the Robonaut 2, a dexterous humanoid robot to be deployed on the International Space Station [37].

As a result of this extended application set, a number of security challenges have arisen for ROS. For instance, [34]:

- 1) Although it is possible to control a networked multi-robot system (swarm), there is no standard approach in ROS to deal with this.
- 2) The importance of real-time communication and control was not originally emphasized.
- 3) The adaptability for non-ideal networks, such as when connectivity suffers from poor quality WiFi and causes information loss or communications delay.
- 4) There are security issues in the basic code of ROS 1.0.

The latter is the most important as it exposes cyber-vulnerability issues, such as:

- 1) **Unencrypted network traffic** - An attacker can view legitimate users' network traffic and record their activities while gathering some confidential information, i.e. perform 'man-in-the-middle' attacks or false data injection. It is also possible for an attacker to use the platform to hijack a third-party communications network.

- 2) **Anonymous graph-type structure** - The anonymity of the ROS publish-subscribe schema makes it easier for an attacker to spoof target systems and applications.
- 3) **Limited integrity checking** - Each node within the ROS graph has limited integrity checking. Consequently, there is no means by which to detect activities from a potentially malicious user, paving the way for an attacker to reverse engineer the system without the host's knowledge.
- 4) **Open topics** - ROS topics are open for subscriptions to any nodes and each node can act as a publisher or subscriber. This makes the system vulnerable to packet sniffers and man-in-the-middle attacks and puts the integrity of the robot's data (which may be on a network) at risk.

The concept of information sharing between various ROS 1.0 client libraries, implemented via XML-RPC suffers from security issues, mainly due to limited integrity checks and the openness of all topics for a subscription.

To highlight the openness and the anonymous nature of ROS, we will discuss the step-by-step process to establish a data connection in ROS. First, we define the role of the ROS Master, which keeps track of the information (note: (which has a known IP address coded into the system)). Second, the publishers inform the master that they are publishing certain topics (e.g. `\cmd_vel`) on a certain local host. Next, the subscriber tells the master that they want to subscribe to `\cmd_vel`, and since the master has been directly informed by the publisher, they can directly pass the information to the subscriber (say, 'I know someones are publishing this topic, and they are located at the local host: 1234'. Having received that information, the subscriber can now establish a peer-to-peer connection to the publisher, and lastly, the publisher sends the data to the subscriber as the connection is established.

As such, these vulnerabilities could lead to serious cyber-threats for any applications in commercial, medical, industrial, and military robots. For instance, data from an arbitrary open topic can be falsified through the injection of malicious data. Sensitive information from any nodes (since all topics are open for subscriptions) can be hacked or reverse engineered without the knowledge of the host (unauthorized access to data).

In addition, nodes can be bombarded by some deceptive messages through the Denial-of-Service (DoS) attacks - a huge amount of data could create significant processing delays, resulting in the inability to process them in real-time. Lastly, ROS systems can be a target for a packet sniffer and man-in-the-middle attacks since there is no way to verify the authenticity of the payload information in transit among nodes [12].

Meanwhile, Within the context of unmanned vehicles, cyber threats can be categorized into several aspects [38], that is, in regards to the availability, confidentiality, and the integrity of the (1) Mission Execution, (2) Communication, (3) Data storage, and (4) the intellectual property of the advanced algorithms. A more detailed explanation can be found in Table I.

In an attempt to raise some awareness on the practicability of cyberattacks on ROS 1.0, the authors in [39] conducted

rigorous penetration testing. They focused on ROS XML-RPC API as their main attack point while introducing two attack tools, namely, **Roschaos** and **ROSPentTo**. Their research clearly demonstrates that it is not difficult to perform cyber-attacks under various modes in ROS, such as to perform (1) false data injection, (2) man-in-the-middle attack, (3) service isolation, (4) malicious parameter update attack. The authors highlight the necessity to have a message definition before injecting false data.

Despite some flaws in the ROS 1.0 API, nonetheless, there are some methods to counter those attacks, such as using **roswtf** command to diagnose potential cyber issues as the system will perform a ROS graph analysis to detect the patterns of potential cyberattacks. For instance, it gives a warning if a listener is isolated from its publisher and if one adds a fake publisher, hides it from the ROS master, the system will also produce a warning. Also, several approaches to enhance security have been introduced, such as using 'Secure ROS' (SROS) and ROS 2.0, which are not susceptible to those malicious attacks.

SROS has been developed to address the shortcomings of the conventional ROS in many ways, by equipping the system with:

- 1) **Transport encryption**, that is, to verify the integrity of the nodes, traffics, and the private connection.
- 2) **Access control**, which can be done by limiting the scope of the node's scope within the ROS graph.
- 3) **Process profile**, meaning to limit the scope of access within the host machine.

For instance, the improvements in **SROS** [40], [41] comes in the form of native Transport Layer Security (TLS) support for all socket-level communication, (2) The introduction of the X.509 Public Key Infrastructure (PKI) certificates, promoting trust, integrity, authenticity as well as (3) The integrity certificate customization (transport encryption), (4) Auditable ROS graph access control, and (5) hardening the process of nodes.

Another version of ROS is **ROS 2.0**, equipped with the security feature of SROS. The system employs the Object Management Group (OMG) consortium Data Distribution Service (DDS) Standard, which can be regarded as an open middleware standard for real-time distributed high-performance communication employing the same publish-subscribe structure in ROS 1.0. Communication through User Datagram Protocol (UDP) is provided by means of eProsima's Fast Real-Time Publish-Subscribe (RTPS) protocol.

There is also a military version of ROS (defence-centric ROS) developed by TARDEC in 2015, known as **ROS-M**, intended for open, modular, robotic architectures with military unique components library [42]. The evolving ROS landscape, such as data encryption at the node level as well as the scope and access of each node play an important role in the future development of ROS.

In line with the vulnerability of ROS, we will discuss some examples of cyberattacks in autonomous systems and their potential countermeasures (see Table I), indicating the practical considerations of cybersecurity.

TABLE I  
LIST OF POTENTIAL CYBER-THREATS IN AUTONOMOUS SYSTEM.

| No | Possible Threats  | Potential Mitigation  |
|----|---|---|
| 1. | GPS/GNSS spoofing (jamming) attacks [43], [44] - availability issue   | Operator behavior pattern using the Hidden Markov model [43], Employing a motion estimator [45], digital map matching and position reset [46], use of compatible receiver, employing environment sensor e.g INS [45].   |
| 2. | Malicious software (Malware) [47] - integrity   | Up-to-date operating systems and anti virus, disconnect drone from the internet (offline) [38].   |
| 3. | Jamming of the wireless communication frequency [48] -availability  | Robustness towards short-term communication loss, using the codes known to both transmitter and receiver, the system transmits radio signal by changing the carrier frequency, employing a large spectral band (i.e., frequency-hopping spread spectrum (FHSS) [49]).   |
| 4. | Command and control data to be captured by an unauthorized personnel [44] (e.g. Iran-US Lockheed Martin RQ-170 Sentinel incident [50])- confidentiality | Software encryption and certified hardware encryption system [50], [51].  |
| 5. | Communication integrity [52] (e.g. overtake control (up-link) and send falsified data (fake position and payload data in the down-link channel)         | Employ variable length signature and data [53], avoid unknown external communication [38].  |
| 6. | Confidentiality of data storage   | Employs user's account to separate access to multiple users, strong password, Role-based access control (RBAC) [54].  |
| 7. | Integrity of data storage   | Using user account privileges, binary data, encryption, signature.  |
| 8. | Confidentiality of the intellect property (IP) [55], [50] e.g. reverse engineering [56]   | Hiding sensitive parts of the code (obfuscation) and steganography (the practice of concealing information within non-secret data) [57], file encryption [58], removing some key parts of the code from the main program and secure them with high level of protection. |

#### IV. AI, MACHINE LEARNING, AND DISTRIBUTED SYSTEMS IN CYBER-PHYSICAL SYSTEMS

Considering numerous potential cyber-threats, some fundamental research questions include how to determine that the system has been compromised, that is, to recognize that something has gone wrong before one can leave the robot in a safe state and restore its functionality. This includes the failure of sub-components and functionality systems, namely, sensors, guidance, and control systems as well as communication links, to name a few.

##### A. Artificial Intelligence and Machine Learning

Artificial Intelligence, often abbreviated as AI, refers to the replication of human intelligence in machines or computer systems, enabling them to perform critical tasks that typically require human intelligence, namely, learning, problem-solving, reasoning, and self-correction [59].

AI encompasses a wide range of techniques and technologies, including machine learning, natural language processing, computer vision, and robotics, among others, to create intelligent systems that can perform tasks autonomously and adapt to new situations.

The systems encompass a wide range of technologies and techniques that enable machines to process information, learn from experience, adapt to new data, and make decisions based on that knowledge. AI systems aim to replicate and, in some cases, exceed human cognitive functions, such as reasoning, problem-solving, perception, and natural language understanding.

Thus, some key components of AI include machine learning, natural language processing, intelligent control, computer vision, robotics, data mining, and speech recognition.

Machine learning can be regarded as a subset of AI, which includes the development of algorithms and statistical models, allowing the systems to improve their performance on a specific task over time based on the given data. This way, machines (computers) can learn patterns from data,

identify trends, and make predictions or decisions without being explicitly programmed [60].

##### B. Potential Cyberthreats

To begin with, we highlight numerous cases in real-life scenarios, as extracted from [61], denoting the importance of security and privacy in robotics as summarised in Table II.

Thus, there are several fundamental steps approach to protecting the system from cyberattacks:

- 1) **Detection of attack**, intended to decide whether or not the system has been compromised and to determine the nature and target of the attack. For instance, the authors in [9] introduced a certain wireless intrusion detection framework to prevent malicious attacks to access networks of communications in networked multi-robot systems.
- 2) **Assessment of attack**, aimed to determine the impacts of attacks on-board the systems. For example, the authors in [72] developed a risk assessment framework for a wireless sensor network in a sensor cloud that utilizes attack graphs.
- 3) **Mission impact assessment**, which is meant to assess the operational capability of the system as demonstrated in [73], where the authors developed a cyber mission impact modeling tool.
- 4) **Report and repair** are the final steps to characterize the nature, extent, and seriousness of the attacks to users.

In what follows, we will discuss some traditional intrusion detection systems (analytical models), widely used for observation or fault detection at the application levels [74]:

- 1) **Distributed filtering**, such as Kalman [75] and particle filters [9], [76], have been widely implemented to predict the presence of potential intruders in any system. For instance, To verify the reported position from GPS, the authors in [76] developed a new framework of wireless intrusion detection for robotic and vehicular networks by

TABLE II  
RELEVANCY OF SECURITY AND PRIVACY IN THE FIELD OF ROBOTICS [61].

| No | Areas  | Examples   |
|----|--|--|
| 1  | Military robots  | UAV systems (e.g. for combat and surveillance) desperately require cyber protection, meaning all communications should be encrypted. However, there was a large portion of military UAVs in 2012 in the US, which had not employed a fully encrypted communication [62].   |
| 2  | Space vehicles   | spacecraft systems must be protected from any potential cyberattack to avoid any non-authorized parties gaining control or sabotaging the entity inside the international space station [62].  |
| 3  | Telehealth and remote surgery robots                       | For the sake of the safety and security of the patient, a remotely operated surgery robot (e.g. DaVinci by Intuitive Surgical Incorporated of Sunnyvale, CA [63]) during an operation must be freed from any unauthorized entity aiming to take over the system, threatening the life of the patient. However, it should be noted that the Interoperability Telesurgery Protocol (ITP) [64], which was originally introduced to secure the interoperability among robotic telesurgery systems, has not used any form of encryption or authentication. This makes the system prone to the man in the middle attack [65].  |
| 4  | Household robots   | Home assisted robots (e.g. Care-O-Bot [66], [67]), equipped with microphones and cameras may collect huge private and confidential data at home, which must be protected. Malicious users may want to take control of the robot and steal a stream of private images and other confidential data.  |
| 5  | Disaster robots  | The role of disaster robots specifically designed to assist with nuclear reactor [68], [69] (e.g. to disconnect nuclear power plant and radioactive materials) is very critical. Hence, it should be protected from any unauthorized malicious intrusion.  |
| 6  | Research and educational robots                            | Many research and educational robots are also vulnerable to cyberattack [70], [12]. For instance, the system may be vulnerable to false data injection to prove a certain behavior to endanger people nearby, e.g. to command the robot to run at full speed despite the presence of humans nearby.  |
| 7  | Humanoid robots (i.e. KAIST Humanoid Robot - 3: HUBO [71]) | Humanoid robots (e.g. Sophia ( <a href="https://www.hansonrobotics.com/sophia/">https://www.hansonrobotics.com/sophia/</a> ) or Josie Pepper ( <a href="https://www.munich-airport.com/hi-i-m-josie-pepper-3613413">https://www.munich-airport.com/hi-i-m-josie-pepper-3613413</a> )) are often required to interact with or entertain general people in public space, such as in the airport to answer passengers' questions. For instance, Munich airport is the first German airport to employ an AI-based humanoid robot, called Josie Pepper (see: <a href="https://www.munich-airport.com/">https://www.munich-airport.com/</a> ). With this role in mind, cyber protection is essential to avoid malicious users who tried to control the robot to make erratic behaviors that could endanger general people. |

means of a particle filtering technique using Received Signal Strength (RSSI) measurements as a metric of detection. The system has two inputs, namely, the reporting position from the GPS and the RSSI measurements used to validate the truthfulness of the reported position. Their research confirms the benefits of distributed particle filtering techniques as the system can verify the reported position within a reasonable amount of time as indicated by FP or TN as a metric of detections.

- 2) **Distributed control** has been widely implemented in autonomous systems [74]. There are several applications of distributed control implemented in autonomous systems, namely, (1) distributed control of manipulators, (2) distributed model predictive control, and (3) distributed control of microgrids. Interested readers are suggested to refer to [74] to gain more insight into detailed applications.
- 3) **Hybrid systems** (e.g. distributed control and filtering) [74]. Given the extensive nature of autonomous systems, hybrid distributed control and filtering with a security perspective still leave rooms to improve. The role of information filtering is undoubtedly important to enhance security and privacy. Some common performance indices include security, stability, and resilience. It is therefore important to get the simultaneous benefits from both state estimations and robust control systems [74]. For instance, in order to regulate active power supply from distributed generators, the authors in [77] introduced a cooperative resilient control supported by a state observation network to monitor the behaviors of distributed generators while isolating the misbehaving nodes. The efficacy of the proposed system is highlighted by means of numerical simulations using the IEEE standard 34-bus test feeder model.

Considering the suitability of the algorithm, it is very useful to consider several criteria such as scalability, robustness

to multiple different sensors, functionality, and the types of parameters as well as the configurations for users, who may not be an expert in that algorithms. For instance, in ROS one possible method to detect any potential intrusions is by investigating networks data analysis (NTA) to investigate communications flows among nodes e.g. bytes transmitted/packets, communication latency, the duration, and the volume of data. The NTA can be used to differentiate between normal and abnormal operating conditions in a wide range of contexts.

While demonstrating some potential benefits, the quality and the robustness of model-based (traditional) intrusion detection methods are pretty much determined by the accuracy of the *assumed mathematical model* of the systems and sensors (see equations (1)). In many cases, those models are not fully available, corrupted, or entirely unavailable due to the complexity of the systems. In fact, in reality, there is *no* perfect mathematical model, and every model contains a certain degree of uncertainties, even for the simplest ones. Also, some estimation algorithms (e.g. Kalman filters) are inherently linear and work best under assumed Gaussian noise only, which are far from the harsh conditions in real life.

Artificial Intelligence, on the other hand, provides unique and more robust solutions compared to traditional model-based systems. The systems have been widely implemented to prevent cyberattacks especially in the context of robotics or unmanned vehicles. There are three most-well known artificial intelligence algorithms to address current research issues in cyber-physical systems with their unique capabilities, namely, knowledge-base (fuzzy systems), self-learning (neural networks), and optimization (genetic algorithms).

For instance, While fuzzy systems (type-1 and type-2) are good at representing human knowledge in the form of its 'If-Then' fuzzy rules, neural networks are well-known for their learning ability (e.g. deep and reinforcement learning, as well as supervised and unsupervised learning). Meanwhile, a genetic algorithm is known for its ability to heuristically

optimize the performance of complex systems, even for non-differentiable systems. Meanwhile, a type-2 Fuzzy system is known for its ability to deal with the footprint-of-uncertainties (FoUs) [78, 79], making a robust system.

For example, the authors in [80] addressed the problem of intermittent denial-of-service (DoS) attacks by introducing a switching-based adaptive fuzzy state estimator. The authors employed convex design conditions to derive the parameters of the system, which guarantee the stability of all closed-loop control signals. In detail, the authors address two major research questions, namely, (1) state estimations in the face of DoS attacks that cause the unavailability of the system states, and (2) how to perform a Lyapunov analysis on active and sleeping intervals of the DoS attack. They introduced a switching-type adaptive state estimator to address the above research questions.

Conceptually, there are at least three types of intrusion detection algorithms, namely,

- 1) **Anomaly-based detection systems**, which work based on the modeling of the statistical behavior of the networks. The system updates its knowledge to adapt to the behavior of the system. Due to the availability of the statistical model of the system, this approach is suitable to detect unknown (new) attacks. To illustrate, the authors in [81] introduced an improved intrusion detection system based on hybrid feature selection and a two-level classifier. In order to reduce the feature size of the training data set, (e.g. the NSL-KDD [82] and UNSW-NB15 [83]), the hybrid feature selection employs three methods, namely, particle swarm optimization, ant colony, and genetic algorithm). The algorithm demonstrates reasonably good performance i.e. 85.8 % accuracy, 86.8 % sensitivity, and 88 % detection rate for the NSL-KDD dataset.
- 2) **Signature-based detection systems**, which can be regarded as the process of building up a database of a *unique signature identifier* so that it can be correctly identified. Although this technique works reasonably well for recurrent attacks and can achieve better accuracy compared to anomaly-based detection systems, it will not be useful to detect new attacks since their signatures have not yet been identified. For example, [84] introduced a parallel processing technique for a small database with the most frequent signature and updating agent. To assist with a simultaneous search of both small databases, containing fewer signatures, and the complimentary database, whose size is larger since it stores old signatures, which are infrequently used; the authors introduced a multi-reading technique. The limitation of this technique is due to the manual update process of the signatures, that is, the administrator has to judge whether or not a signature is harmful before adding it to the database. Also, while the technique is not available in all hosts, it may be suffering from compatibility issues since not every type of IDS can support it.
- 3) **Specification-based detection**, which combines the benefits of both signature-based and anomaly-based de-

tection by manually specifying certain behavioral specifications used as a basis of attack. For instance, Hwang in [85] introduced a hybrid intrusion detection system leveraging the benefits of the low false-positive rate of the signature-based intrusion detection system (IDS) and the ability of the anomaly-based detection system to prevent new (unknown) attacks. By means of anomalous traffic episodes from the internet connections, the authors introduced a system that can detect anomalies outside the capabilities of the signature-based SNORT system as in [86], [87]. The efficacy of the proposed ID system was investigated using real-time internet trace data supported with 10 days of MIT/Lincoln Laboratory (MIT/LL) attack data set. The system demonstrated a 60 % detection rate compared to 30 % and 22 % for SNORT and Bro system [88], respectively; supported with a reasonably low false positive alarm of 3 %. In fact, the signatures generated by the system have enhanced the performance of the SNORT by 33 %. Their research demonstrates the effectiveness and the validity of the hybrid system supported by data mining and signature generation over the internet connection episodes.

Addressing the demands of achieving a robust and resilient control, Linda et al. introduced a new robust security system using Type-2 fuzzy systems due to the ability of the system to accommodate the footprint-of-Uncertainties (FoUs). The learning algorithm is due to rule extraction via the online nearest neighbor clustering technique. The system provides the basis for anomaly basis intrusion detection systems while it is also capable of complying with constrained computational requirements for low-cost embedded networks. In an attempt to emulate a cyberattack environment, the authors employed Nmap (a network scanning tool to identify host, scan ports, operating systems, and to decide applications, listening to one open port) and Nessus (a network scanning tool with auditing capabilities e.g. vulnerability and profiling information) software. Their research indicates that the system achieves 98.84 % of classification rate with 0.0 % of a false-negative and 1.31 % of false-positive rates.

Distinguishing an overlapping between the threat and the legitimate data, the authors in [89] introduced a wavelet-based multiscale Hebbian learning approach in neural networks. This way, the weights, and bias are updated with respect to the multiscale approach. The authors employed UNSW-NB15 for their experimental dataset and compared the efficacy of their technique with respect to the traditional gradient descent-based learning technique. Their research indicates that while detection accuracy of single scale Hebbian-based-NN and gradient descent-based NN is of comparable magnitude, the proposed system is capable of distinguishing the non-linear and overlapped feature space of cyber-world data. Overall, the system demonstrated improved performance with a true negative of 95 % and a true positive rate of 73 %. A relatively low true positive rate results in improved precision and accuracy. Their proposed approach is also effective to reduce false positive and negative rates at the same time.

To reconstruct and compensate cyberattacks in the forward link of a nonlinear system, the authors in [90] introduced

a new hybrid of intelligent control technique by means of neural networks and a classical control system using a variable structure (VS) control technique. While the purpose of the employing non-linear VS control technique was to guarantee both the stability and the robustness of the closed-loop system, the online neural networks trained using Lyapunov-based adaptation law were to achieve an intelligent estimator to estimate the network attack pattern. It is evident that the proposed method was robust not only against cyberattacks but also with respect to external disturbances affecting the system.

Overcoming false data injection attacks in industrial control systems, the authors in [91] introduced an artificial neural network-based identifier. The data was split into 65 % for training, 15 % for validation, and 20 % for testing. While the training was performed in a supervised manner using a non-linear regression technique to abstract information and to detect any potential attacks, the testing phase is meant to highlight the performance of the system. On-line data streams were directly obtained from the plant, which was first used to train the neural networks for attack identifications while different types of attacks were injected into the system to study the performance of the system. Their research demonstrates promising detection accuracy of the proposed security system.

Prioritizing alerts, Newcomb in [92] presented a new cybersecurity approach, namely, the FLUF (Fuzzy Logic Utility Framework) technique to support computer networks in making a defense decision. Taking into account risk management techniques from both offensive and defensive perspectives while accommodating human expertise, the author developed a fuzzy rule-based to assist cyber defenders with informed decision support to improve their efficiency while increasing mission assurance by first focusing on the most severe alert of cyber intrusion detection. Current FLUF implemented components from CARVER (Critically, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability) as well as the Risk Management Framework (RMF) to rate the feasibility of an eligible target.

Concerning security in modern vehicles, especially in the area of in-vehicle networks, the authors in [93] introduced a new intrusion detection algorithm using fuzzy systems to detect several different types of attacks (i.e. denial of service attack, fuzzy attack by injecting messages of totally random CAN ID and DATA every 0.5 milliseconds, and false data injection to the gear and the rpm) to the Controller Area Network (CAN) protocol (a subset of ISO/OSI stack in levels 1 and 2). The fuzzy logic algorithm was employed to differentiate between the legitimate CAN packets and the malicious 'injected' ones. To highlight the efficacy of the proposed system, the authors employed real-world data embedded in the CAN packets. Their research indicates that the proposed method can achieve a precision from 0.85 to 1.

Motivated by the need to improve resiliency and state-awareness, the authors in [94] developed a new control system, namely, a 'fuzzy-neural data fusion engine' (FN-DFE). The proposed control system consists of three layers, that is, (1) threshold-based alarms, (2) behavior detector using a self-organizing fuzzy system, (3) modeling and prediction based on an artificial neural network. The enhanced state awareness of

the system can be achieved by fusing input data from multiple sources to achieve robust anomaly indicators, in addition to the signal prediction performed by neural networks. Their experimental outcomes indicate that the proposed FNDFE technique demonstrates its ability to timely monitor the performance of the plant, in addition to its capability of performing accurate anomaly detection. The system can identify intrusive behaviors much earlier than the traditional threshold-based alarm systems.

Addressing research questions in denial of service (DoS) attacks, the authors in [95] employed dual deep learning neural network architecture based on convolution layers. Their research novelty comes in the form of the reinforcement of the input vector with its cluster evaluation. Their research also indicates a significant increase in the processing speed, making it possible to detect attacks in busy corporate networks. For instance, the processing speed of 32,768 windows relating to 523 s of traffic can be performed within 1.8s to 2s. When it comes to the accuracy of the abnormal packet detection, the system can achieve a reasonably high figure of 87 %. Overall, their research demonstrates the possibility to achieve an intelligent network firewall to achieve information security of the enterprise.

Considering the importance of a secure healthcare industry, Li et al. in [96], introduced a new security system, namely, 'Medical Fuzzy Alarm Filter' (MFAF). The proposed cybersecurity system leverages the benefits of knowledge-based fuzzy inference systems to handle the vagueness and imprecision in the data. The algorithm contains two major phases for generating fuzzy rules from numerical data, that is, to transform a pattern space into fuzzy subspaces, and secondly to determine fuzzy 'if-then' rule for each fuzzy subspace. The authors conducted two major experiments to investigate the efficacy of the system, by means of simulations and real network environments. Their experimental results suggest the practicality of the proposed algorithm to work in real medical environments. Also, the system can achieve better accuracy compared to traditional supervised learning algorithms.

In response to the monumental growth of internet applications, the authors in [97] introduced an anomaly detection model based on multiple deep neural network structures, such as convolution neural networks, autoencoders, and recurrent neural networks. To gauge the performance of the proposed algorithm, the authors employed multiple conventional machine learning algorithms (e.g. an extreme learning technique, the nearest neighbor method, a decision-tree approach, a random-forest procedure and, a support vector machine concept as well as a naive-bays technique and a quadratic discriminant analysis). To highlight the benefits of the system, the authors employed a confusion matrix, presenting the performance of the system in terms of true positive, false positive, true negative, and false negative. Their research highlights promising results for the real-time applications of deep learning in anomaly detection systems (i.e., 85 % and 89 % for both deep convolutional neural networks (DCNN), a special class of neural networks to handle high dimensional data supported by some spatial semantics, and long short term memory (LSTM)



models, which can be regarded as a special recurrent neural network (RNN) architecture).

Focusing on vulnerability management, the authors in [98] developed an optimization framework based on genetic algorithms to manage the security by means of the Open Source Testing Methodology Manual (OSSTMM). The genetic algorithm is meant to optimize a certain cost function, accommodating the security level and some specifications from the clients (e.g. maximum deployment costs). The authors employed two OSSTMM indices, namely 'the Actual Security' and the True Protection' to validate the benefits of the proposed approach. The algorithm was also validated based on a real security evaluator scenario. The effectiveness of the proposed system as an offline regulator in a decision support system was demonstrated through numerical simulation results.

Considering the benefits of state estimators, Zhang et al. in [99] implemented a Takagi-Sugeno fuzzy model to predict the behavior of a non-linear security system consisting of a set of wireless sensors supported by a communication channel. The authors studied the effects of multiple phenomena in autonomous system such as sensor saturations, signal quantization, packet dropouts, and medium access constraints. They developed a certain framework to achieve an asymptotic stability convergence of the filtering error in the sense of mean square, in addition to the prescribed  $H_\infty$  performance level. This way, the gain of the filter was computed by solving a convex optimization problem. A case study on the network truck-trailer system was implemented to highlight the efficacy of the estimator design.

Aiming for safeguarding the trusted operation of robotic vehicles while addressing the shortcomings of Robot Operating System (ROS), Santoso and Finn in [100] developed a new cybersecurity system based on the concept of deep learning convolutional neural network. ROS is a well-known middleware platform widely used in both civilian and military robots. The authors conducted real-time cyberattack experiment to study the operation of the GVR-BOT ground vehicle, a replicate of the US Army ground robot, under man-in-the-middle cyberattacks and to exploit the vulnerability of the Robot Operating System (ROS) employed in its onboard computer. The normalised time-series data was converted into RGB or grayscale images to train the CNN system to learn the patterns of the robot under both the legitimate and malicious operations. The authors conducted statistical analysis to highlight the efficacy of the proposed system. It turns out that the system is quite effective since it can achieve a reasonably high accuracy  $\geq 99\%$  and substantially small false positive rates  $\leq 2$  supported with minimum detection times. The authors also compare the benefits of the algorithm with similar techniques.

Jahromi et al. in [101] introduced a new framework to address security issues in IoT-enabled cyber-physical systems. The authors developed a two-level attack detection mechanism suitable for imbalanced data in industrial control systems. While the first stage includes a decision tree supported by a deep representation learning model to deal with attack-imbalanced environments in industrial control systems, the

second stage consists of an ensemble neural network to facilitate attack attribution. To study the efficacy of the proposed system, the authors employed a real-world dataset from a gas pipeline and water treatment system. Despite the complexity of the proposed model, the complexity of the training and testing phases are similar to other deep neural network systems in the literature. Their research indicates the superiority of their model against the proposed counterpart as it demonstrates better recall and f-measure than earlier work.

In what follows, we briefly summarize some applications of AI and machine learning algorithms, in addition to their potential benefits (see Table III).

## V. DISCUSSION AND POTENTIAL RESEARCH AVENUES

This section will discuss some potential research challenges in the development of AI and machine learning algorithms for robotics and autonomous system.

### A. Security and Protection in Data and Communication Networks

While in the past researchers merely focused on the capability and the functionality of robots, currently privacy and security are also important considerations. For instance, the initial development of ROS 1.0 has not seriously taken privacy and security issues into account i.e. ROS network traffic remains unencrypted with limited integrity check on the received packet other than some basic messages and API call identity.

Addressing security and privacy, it is highly important to encode the message during the transmission and communication process in a way that the information is only available to the authorized parties. This leads to the first research challenge, namely, the development of efficient and robust encryption algorithms to avoid any intrusions at various layers (e.g. brute force attacks). Some current state-of-the-art developments of cutting-edge encryption keys include symmetric-key algorithms [106], public key cryptography [107], and distance-based encryption [108], to name a few. In this avenue, the research challenge is to ensure the integrity, confidentiality, and availability of data, while harnessing the power of AI to proactively detect, respond to, and adapt to emerging threats in real-time.

### B. AI-enhanced Bio-Inspired Fault Detection System

While traditional cybersecurity measures often rely on pre-defined rules and signatures, which are inadequate in addressing the rapidly evolving threat landscape, currently, there is a demand for a bio-inspired fault detection system that draws inspiration from biological systems to effectively and autonomously detect, respond to, and mitigate cyber threats and vulnerabilities.

Under this research theme, we address a fundamental research question on how to effectively design and implement a bio-inspired fault detection systems in the realm of cybersecurity for robotics and autonomous systems to enhance their security, resilience, and adaptability in the face of evolving

TABLE III  
SUMMARY OF AI AND MACHINE LEARNING FRAMEWORKS FOR NETWORK TRAFFIC ANALYSIS IN CYBER-PHYSICAL SYSTEMS

| No  | Algorithms  | Purposes  | Benefits   |
|-----|---|---|--|
| 1.  | Fuzzy Logic (fuzzy-NN) Algorithms [93]  | To detect four different types of attacks targeting the controller area network (CAN) protocol  | High accuracy (0.85-1).  |
| 2.  | Fuzzy-Neural Data Fusion Engine (FN-DEFE) [94]  | To develop a robust state monitoring to identify system behaviors in the face of faulty. The system consists of three layers, namely, (1) traditional threshold-based alarm, (2) fuzzy logic-based anonymous detection, (3) ANN-based for modeling and prediction | Timely plant monitoring and anomaly detection capabilities. Earlier detection of intrusive behaviors than conventional threshold-based alarm systems.                      |
| 3.  | Dual deep learning NN with clustering technique [95]  | To detect DoS attacks   | Reasonably high accuracy of 87 %, suitability for real-time operation.   |
| 4.  | Knowledge-based fuzzy if-then rules [96]  | To introduce a medical fuzzy alarm filter (MFA filter) for healthcare environments which can handle the vagueness and imprecision   | Better accuracy compared to traditional supervised algorithms, practical (real-time) benefits.   |
| 5.  | Convolution neural networks (CNN), autoencoder and recurrent neural networks [97]   | To investigate the suitability of deep learning for anomaly-based intrusion detection systems   | Both NN models demonstrated exceptional performance with 85 % and 89 % accuracy on test data-set demonstrating the viability of the system for cybersecurity applications. |
| 6.  | Adaptive Neuro-Fuzzy Inference System (ANFIS) with a series of pages route analysis, network analysis, feature selection, and attack classification phases [102]  | To allow the desired access to the system by investigating network traffic and the previous record  | Improve accuracy for classification of different types of attacks. Reliable systems.   |
| 7.  | Genetic algorithm to extract principal component analysis [103]   | To enhance the security of the network  | High detection rates while speeding up the processing.   |
| 8.  | Genetic algorithm and the Open Source Security Testing Methodology (OSSTMM) [98]  | To introduce an optimization framework for controlling a CPS system at the security level.  | The system is suitable for the management of vulnerability.  |
| 9.  | TS Fuzzy-Model-Based-Filtering Technique [99]   | To model a class of non-linear CPS systems. The physical plan is measured by wireless sensor networks, communicating with a remote estimator via a communication channel.   | The accuracy and robustness in the face of non-linearity.  |
| 10. | Naive Bayes, $k$ -nearest neighbor, decision tree, and support vector machine [104]   | To investigate a multivariate analysis of data of video calls   | An accuracy of 81 % for bandwidth prediction and 60 % for destination prediction.  |
| 11. | FLUF (Fuzzy Logic Utility Framework) [92]   | To prioritize intrusion detection alert based on fuzzy systems  | Improved efficiency and increased mission accuracy by prioritizing the urgency of the alert.   |
| 12. | A Hybrid of a traditional (variable structure) control method and an intelligent control approach (neural network) for reconstruction and compensation of cyberattacks [90]   | To guarantee the stability of the closed-loop control system when attacks happen  | Robustness against cyberattacks and disturbances.  |
| 13. | Artificial Neural Networks [91]   | To identify potential false data injection attacks (FDIA)   | Promising detection accuracy based on the experimental data.   |
| 14. | Wavelet-based multi-scale Hebbian neural network [89]   | To differentiate overlapping classification boundaries between the threat and legitimate data over feature space  | Based on the UNSW-NB15 dataset, the system shows promising results for the gradient descent-based learning technique.  |
| 15. | Type-2 Fuzzy system [20]  | To leverage the advantage of Type-2 fuzzy in accommodating the Footprint of Uncertainties (FoU), that is, to develop a robust anomaly detection of CPS system.  | a robust and accurate system (i.e., the typical performance of 98.84 % correct classification rate with 0 % false negative, and 1.31 % false-positive rates.               |
| 16. | Convolutional Neural Networks supported by a voting filter [105] and [100]  | to develop a robust data-driven cyber intrusion detection systems to accommodate the shortcomings of ROS  | A robust and accurate system with reasonably high accuracy, substantially small false positive rates and rapid detection time.   |
| 17. | Two-level attack detection mechanism for imbalanced data in industrial control systems, namely, a decision tree supported by a deep representation learning model, the second stage consists of an ensemble neural network to facilitate attack attribution | to address security issues in IoT-enabled cyber-physical systems  | A robust system with better recall and f-measure compared to the previous work.  |

threats? It includes recognizing any potential attacks (intrusion) before isolating the system and leaving the robot in a safe state by maintaining its functionality in the face of failure.

Under the umbrella of AI, there are multiple fault detection algorithms with their unique capabilities. In this review, we narrow them down into three major techniques based on their popularity and capability, namely, neural networks with their ability to learn, fuzzy systems with their unique capability to represent the vagueness in real-life in terms of fuzzy knowledge and the footprint of uncertainties (FoUs), and genetic algorithms with their optimization feature. There are also multiple hybrid combinations among those three intelligent algorithms, such as neuro-fuzzy systems, combining the benefits of learning and knowledge-based systems, GE-fuzzy systems, taking the advantage of optimization and knowledge-based techniques.

1) *Fuzzy Systems*: Imitating the way human reasons, fuzzy systems due to Zadeh [79] is an approximate reasoning, deriving the conclusion based on a set of expert users manifested in the set of fuzzy linguistic ‘If-Then’ rules, namely,

$$\mathbb{R}^i : \text{If } x_1^i \text{ is } \mu_1^i \text{ AND } x_2^i \text{ is } \mu_2^i \dots \text{AND } x_n^i \text{ is } \mu_n^i \quad (3)$$

**Then**  $y_i := f(x_1, x_2, \dots, x_n)$ ,

where  $x_j^i = [x_1^i \ x_2^i \ \dots \ x_n^i]^T$  denotes the input vectors for the  $j$ th input,  $\mu_j^i = [\mu_1^i, \mu_2^i, \dots, \mu_m^i]^T$  indicates the fuzzy membership functions for  $i$ th rule,  $f(\cdot)$  indicates a certain function, representing the output of the Takagi-Sugeno fuzzy system while for Mamdani counterpart it can be replaced by a set of output membership functions, and  $y$  is the output of the  $i$ th fuzzy rule.

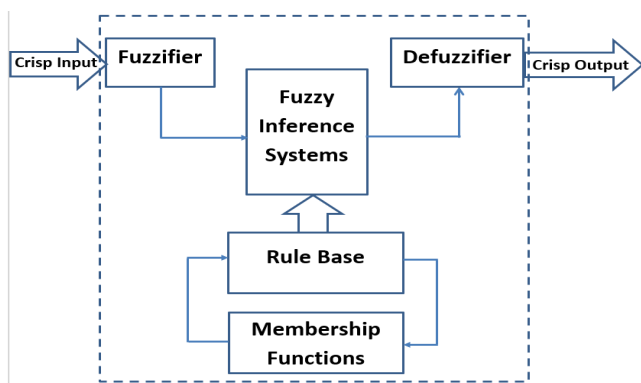


Fig. 3. Block diagram of fuzzy inference system (FIS), showing three major steps in fuzzy systems, namely, fuzzification, defuzzification, inference engine.

The system consists of three fundamental steps (see Fig. 3), namely fuzzification (a mapping from crisp inputs into fuzzy sets), rule-based fuzzy inference engine, and defuzzification technique (transforming fuzzy values into real variables). The system allows for some simple interactions as well as a direct interpretation of the results.

Fuzzy logic’s ability to handle uncertainty and imprecision makes it a valuable tool in cybersecurity for making more informed and context-aware security decisions. It is particularly useful in scenarios where binary decisions may not be adequate for assessing and responding to complex security situations.

- **Intrusion Detection Systems (IDS)**: Fuzzy logic can be used in IDS [92] to evaluate network traffic and identify suspicious patterns. Fuzzy rules can help analyze data and generate alerts by considering the degree of membership of data points in various categories, allowing for a more nuanced assessment of potential threats.
- **Access Control**: Fuzzy logic can improve access control mechanisms [109] by considering the uncertainty in identity verification. It can facilitate adaptive and flexible access policies based on the degree of certainty in user identity.
- **Anomaly Detection**: Fuzzy logic can be applied in anomaly detection systems [94] to assess the deviation of observed behavior from a baseline. By using fuzzy membership functions, it is possible to quantify the degree of abnormality in system behavior.
- **Risk Assessment**: Fuzzy logic can be employed in risk assessment models to evaluate the likelihood and impact of security incidents [110]. It allows for a more granular assessment of risk by considering multiple factors with varying degrees of importance.
- **Password Strength Assessment**: Fuzzy systems can be used to assess password strength [58] by considering various criteria such as length, character diversity, and entropy. It can provide a more nuanced evaluation of password security.

Addressing the requirements of accommodating the uncertainties, Zadeh [79] introduced Type-2 fuzzy systems (an extension of the type-1 fuzzy system) by introducing a new dimension called *the footprint-of-uncertainties (FoUs)* in both the antecedent and consequent parts. Despite being more noise-tolerant, the Type-2 fuzzy system is more computationally intensive than the type-1 counterparts.

One potential challenge in implementing fuzzy systems in robotics and autonomous system is due to the generation of fuzzy rules and membership functions (MFs), especially for systems with many variables [111]. Although it is possible to use expert knowledge to set fuzzy rules, especially for a system with only a few variables, for large-scale systems, the process may be very tedious, inefficient, or next to impossible.

This will lead to the demand of having an automatic tuning system (e.g.,  $C$ -means clustering or hybrid approach with neural networks). It is also possible to solve the optimization problem using GA given the nature of the fuzzy systems as a search algorithm in a high order of dimensional space, that is to work out the optimal solution over a hypersurface.

2) *Artificial Neural Networks*: Another algorithm worth considering is Artificial Neural Networks (ANNs). Replicating the way the human brain operates, ANN systems (see Fig. 4) can be seen as interconnected neurons (represented by tuneable weights), exchanging messages to each other. The system comes under various architectures, such as feedforward, recurrent, and feedforward radial basis function (RBF), to name a few.

Neural networks offer the potential to provide adaptive, real-time cybersecurity for robotics, which is essential given the increasing integration of robots and autonomous systems into various industries. They can identify and respond to threats

with greater speed and accuracy, safeguarding the integrity and operation of these systems.

They offer the capability to analyze vast amounts of data, detect anomalies, and respond to threats in real-time. Several ways neural networks are used in cybersecurity for robotics:

- **Intrusion Detection:** Neural networks can be used to detect anomalies in network traffic within robotic systems. They learn to recognize normal patterns and identify deviations that could signify a cyberattack or intrusion [97], [105], [100].
- **Behavior Analysis:** Neural networks can analyze the behavior of cyber-physical systems to identify unusual or malicious activities [112]. By monitoring the activities and actions of the systems, they can detect unauthorized or anomalous behavior.
- **Malware Detection:** Neural networks can be used to identify malware or suspicious code within the software used by robotic systems. They can learn to recognize patterns and signatures associated with known malware [113].
- **Anomaly Detection:** Neural networks are effective at spotting anomalies in sensor data, which is crucial for robotic systems [105], [100]. They can identify unusual sensor readings that could indicate a malfunction or tampering.
- **Password Authentication:** Neural networks can enhance authentication and access control mechanisms by evaluating the strength of passwords and user authentication, helping to prevent unauthorized access [114].

One major advantage of the system is its suitability for highly parallel intelligent learning. Second, the system is suitable to tackle multiple challenging optimization problems beyond linear programming. While the NN system is sufficiently robust and capable, setting up the appropriate number of layers and neurons is somewhat challenging [115]. This way, the concept of simulated annealing comes into the picture as it is often used to train the system and to perturb the ANN weights by random values in order to avoid getting trapped in the local minima. Interested readers in the area of deep learning are recommended to refer to [97].

Generally speaking, there are at least three learning strategies normally used to train neural network systems, such as:

- 1) **Supervised learning** (e.g. [116] is a learning method when the system is trained using the input/output pairs provided by external/ internal resources. There are many applications of supervised learning to address security issues, namely,
  - **Malware Detection:** Supervised learning algorithms can be trained to recognize known malware patterns and behaviors [117]. They can analyze software running on robotic systems and identify malicious code or unauthorized software.
  - **Intrusion Detection:** Supervised learning models can monitor network traffic and system logs to detect unauthorized access and suspicious activities e.g. [118]. By training on labeled datasets of normal

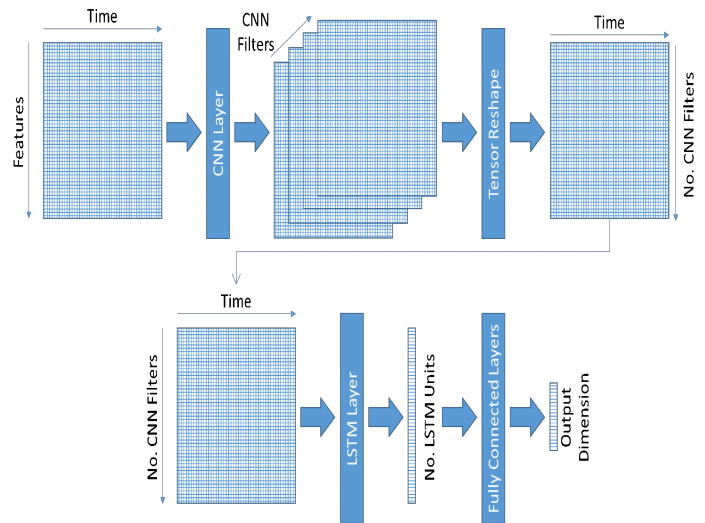


Fig. 4. (a) Deep learning convolutional neural networks (see [105], [100]) While input layers (input nodes) represent the input variables of interest (e.g., traffic data, tracking error, and received signal strength), the output layers are related to output variables of interests, namely, the position and velocity of the robots as well as detection rates. Each node is connected to other nodes via a certain weight before being passed to an activation function, (b) Convolutional Neural-Network with Long-Short Term Memory for classification.

and malicious network traffic, these models can identify intrusions and cyberattacks.

- **Anomaly Detection:** Supervised learning can be used to create models that define the normal behavior of systems [119]. Any deviations from this norm can trigger alerts and potential security responses, allowing for the detection of both known and unknown threats.

2) **Unsupervised learning** (e.g. [120]) is a training method to teach the NN to respond to a certain pattern in the absence of the output examples. Some applications of unsupervised learning in this context include:

- **Anomaly Detection:** Unsupervised learning can identify anomalies in robotic system behavior and network traffic without the need for labeled data [121]. It's particularly useful for discovering previously unknown threats and unusual patterns, which might go unnoticed by traditional supervised methods.
- **Intrusion Detection:** Unsupervised learning models can analyze system logs, network traffic [122], and sensor data to uncover suspicious activities that don't conform to normal behavior. This is especially valuable for detecting novel attack vectors.
- **Network Traffic Analysis:** Unsupervised learning can cluster network traffic data to identify unusual traffic patterns or group similar network behavior, helping to detect unauthorized access or attacks [123].

3) **Reinforcement learning** (e.g. [124]) can be considered as a combination of supervised and unsupervised learnings. Adopting the evolutionary concept, the neural network systems can undergo both structural and

parametric changes as the systems continuously evolve. Some applications of reinforcement learning include:

- **Adaptive Security Policies:** Reinforcement Learning can be used to dynamically adjust security policies and configurations based on changing threat landscapes and system vulnerabilities [125]. It allows the systems to respond in real-time to emerging threats and adapt their security measures accordingly.
- **Threat Response:** Reinforcement Learning models can be trained to determine the most effective and appropriate responses to detected cyber threats [126], ranging from isolating compromised components to initiating countermeasures.
- **Intrusion Response:** Reinforcement learning can facilitate the development of adaptive reinforcement learning [127], allowing the systems to effectively defend against cyberattacks, reducing the potential damage.

Reinforcement learning in cybersecurity enables the systems to learn from experience, adapt to new threats, and make autonomous decisions, making them more resilient to evolving cyber threats and enhancing overall security posture. Considering the applications of multiple machine learning algorithms in cybersecurity, interested readers are referred to [128].

- 4) **Adversarial learning** is a machine learning technique aiming for enhancing the robustness of the model against adversarial attacks i.e. intentional attacks to manipulate input data in a way that they lead to corrupted or unexpected model outputs in order to exploit the vulnerabilities in machine learning models [129].

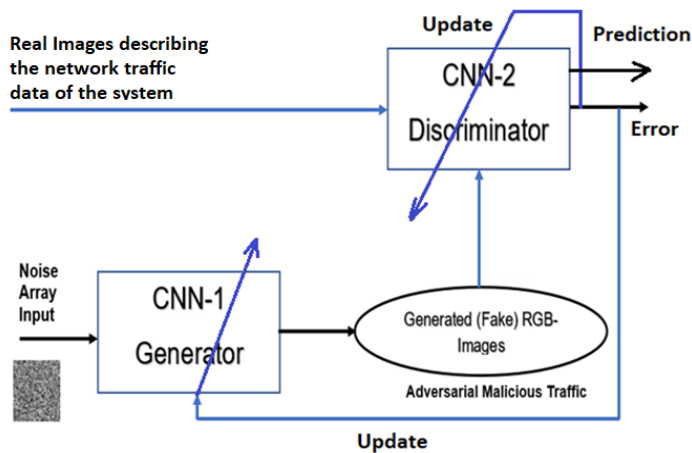


Fig. 5. Generative Adversarial Learning involving two competing CNNs.

In adversarial learning, there are two competing neural networks, referred to as the generator and the discriminator (see Fig. 5). This approach is particularly common in the context of generative models and is used to create realistic (synthetic) data, such as images, audio, or text. This way, a model can be trained to be robust against adversarial attacks. Adversarial attacks involve intentionally manipulating input data in such a way that it

leads to incorrect or unexpected model outputs. These attacks are typically designed to exploit vulnerabilities in machine learning models.

In this avenue, the term “adversarial” refers to the adversarial relationship between the defender (the machine learning model) and the attacker (the entity trying to manipulate the model’s behavior). The purpose of this technique is to improve the robustness of machine learning models for applications where security and reliability are critical, such as in robotics, autonomous systems, and critical infrastructures.

- 3) **Genetic Algorithms:** Mimicking the concept of natural ‘Darwinian’ evolution, GA is a heuristic optimization method introduced by Holland [130]. Owing to the concept of the survival of the fittest, the algorithm works by evolving the population (candidate of solutions) to find the strongest candidate (as an optimum solution) which can emerge via mutation and crossover.

Genetic algorithms (GAs) have gained attention in the field of cybersecurity as a means to address complex optimization and decision-making problems. They are inspired by the process of natural selection and evolution and can be applied to various aspects of cybersecurity. Here’s an overview of how genetic algorithms are used in cybersecurity:

- **Decrypting User’s Personal Information:** Genetic algorithms can be used to optimize the search for user’s personal information [131]. By evolving a population of potential passwords, the algorithm can improve its chances of finding the correct password faster, especially when dealing with strong and complex passwords.
- **Intrusion Detection:** GAs can aid in the development of intrusion detection systems. They can evolve rules or heuristics for detecting suspicious activities or patterns in network traffic, making the system more adaptable to new attack techniques [132].
- **Botnet Detection:** GAs can be used to identify and track the behavior of botnets. They can evolve algorithms that recognize botnet traffic patterns and facilitate early detection and mitigation [133].

In GA, the information is encoded in the chromosomes, comprising hundreds or thousands of genes as a part of the DNA segment. For instance, humans have 23 pairs of chromosomes (46 chromosomes). Through an iterative process, each time the mutation process occurs, an element will be adjusted by one step random integer inside its range while an efficient search is facilitated through crossover (to explore the search space) and mutation (to facilitate genetic diversity) to guide the system to move into a new region.

While it is possible to employ crossover and mutation with a fixed probability, it is highly recommended to employ a variable rate (starting with a higher crossover value before increasing the mutation rate towards the end of the process) to lead to optimum results. One potential research challenge in GA is related to how to avoid getting stuck in local optima (although this drawback can be addressed through the crossover process).

### C. Intelligent Learning: Structural and Parametric Adaptation Mechanisms

Intelligent systems such as fuzzy systems and neural networks require rigorous training (online and offline) before they can be purposefully implemented to model the complex dynamics of the systems. In the context of security, the problem statement is related to the development of intelligent learning systems, incorporating both structural and parametric learning, ensuring the resilience and adaptability of cybersecurity defences in the face of evolving threat landscape. As such, the goal is to investigate how these learning systems can be harnessed to provide greater resilience and adaptability to protect robotics against constantly evolving cyber threats. Self-learning systems must adapt in real-time to detect and respond to novel attacks. Ensuring that the security systems can continuously learn and improve while avoiding false positives and negatives is a challenge.

To make the most of it, it is also possible to combine such systems. For instance, combining fuzzy systems and neural networks to achieve and adaptive systems that can perform automatic learning while keeping the knowledge in the form of 'if-then' fuzzy rules. This way, one can facilitate both structural and parametric learning.

Structural learning can be performed by modifying the structure of the knowledge-based fuzzy system itself (e.g. by adding new rules or removing the unnecessary old rules that have little relevance to the dynamics of the systems), while parametric learning is related to the optimization of each fuzzy parameters (e.g. in the membership functions and the consequent parts).

Such systems can mimic the way human reasons. For instance, as we learn every day, we are constantly bombarded by millions of information through our sensory systems (i.e. auditory, visual, smell, tactile, etc). In fact, not every piece of information is relevant to us, and only a small portion of the information we receive is useful.

This way, our brain acts as a filter to remove irrelevant data while keeping the most relevant information in our short-term memory so that it can be easily recalled in the future. After a while, if the information may be archived in the long-term memory or completely removed if it is getting progressively less relevant.

The process is iterative and it also somehow mimics the nature of biological evolutions, that is the survival of the fittest. It means, in the end, only the information that is most relevant to describe the dynamics of the system will survive while the rest will be gradually replaced.

Unlike some traditional estimation techniques (i.e. Kalman and particle filters) relying on the accuracy of the assumed mathematical models, AI techniques can give an accurate prediction without the need to obtain the system models first, saving time and costs. Moreover, advancements in Type-2 fuzzy systems could lead to substantially more robust security systems due to the nature of Type-2 fuzzy systems to accommodate the footprint-of-uncertainties (FoU), making it suitable to predict the uncertain dynamics of non-linear systems. This way, we speculate that in the future people will heavily rely

on intelligent systems to prevent autonomous systems from potential cyberattacks.

### D. Accelerated Learning Duration

Another potential research avenue in the area of machine learning and cybersecurity is due to processing time. While it is necessary to learn as quickly and as efficiently as possible, for some complex algorithms, the process may take longer, which in turn may suppress the accuracy and increase the false-positive rates, especially for the large data streams. This will decrease the capabilities and the values of the systems, especially when high detection bandwidth is required. Thus one need to address an important research question of how AI technologies can be harnessed to expedite the learning and adaptation time, ensuring faster and more effective responses to emerging threats and vulnerabilities?"

Addressing this potential research gap, it is very important to develop machine learning algorithms that can avoid overfitting, a common problem of the increasing complexity of the model of the system to accommodate all variations in the traffic data (i.e., the extraneous superfluous incoming data). This leads to the development of efficient pruning techniques (e.g. rule recall mechanisms in fuzzy systems [78] or node recall mechanism in neural networks [134]) in order to increase the computational efficiency while enhancing the practicality (real-time values) of the algorithms.

### E. Uncertainties in Data Distribution

The nature of robotics and autonomous system is marked by uncertainties in data and measurements. Because there could be a potential mismatch in the data structure, i.e. the I/O data may not follow a certain predictable distribution. Therefore, it is also important to achieve a robust security algorithm, that is, a detection system that can work well in the face of large uncertainties, in the presence of incoming data (drifting) that may not lead to new knowledge of the existing model.

These uncertainties arise from various sources and can impact the overall safety, privacy, and functionality of robotic systems. Some key uncertainties (variability) in data distribution may be due to diverse sources, such as sensors (e.g. LiDAR) and their malfunctions (e.g. due to callibrations), environments (lighting, weather, obstacles), adversarial attacks (sensor spoofing and jamming), data privacy (the need to protect sensitive information while performing the tasks), communication uncertainties (e.g. latency, packet loss, or interference).

Addressing this issue, one need to develop a robust system that can effectively handle uncertainties in data distribution while ensuring the security and reliability of these systems. Thus, the research avenue is related to designing a robust security system, that could deal with uncertainties while filtering out some irrelevant superfluous incoming data. As such, Type-2 fuzzy systems may be desirable due to their ability of the system to accommodate the footprint-of-uncertainties [78].

### F. Stability and Plasticity Dilemma

In self-learning, the stability and plasticity dilemma is an interesting research question [135]. The idea is to achieve

a delicate balance between those two conflicting constraints, especially in parallel and distributed systems [136]. While plasticity is required to acquire (integrate) new knowledge, stability is needed to avoid forgetting the previous knowledge. However, the implication of having too much plasticity is to constantly forget the previously acquired knowledge while too much stability will reduce the learning efficiency.

It will be very difficult to add new knowledge in a very stable system. In line with the research question in cyber-physical systems, one needs to design a robust and efficient learning system such that the degree of stability and plasticity is the right one in order to maximize the detection rate while minimizing all false alarms. One needs to achieve sufficient robust learning capability in the proposed system such that catastrophic forgetting (losing previously learned information as soon as new information has arrived) can be avoided. Thus, current research question is related to how to strike a delicate balance between stability and plasticity while ensure security and remaining adaptable to dynamic and evolving threats?

## VI. CONCLUSION

By way of conclusion, we have presented a rigorous overview of security aspects in robotic and autonomous systems, especially when it comes to the role of machine learning in preventing cyber attacks, and its comparison with respect to model-based conventional algorithms. There are big opportunities for research in this area since most systems are not well-prepared (e.g. poor protection in ROS systems, unencrypted communications, etc.).

Thus, one main intention of this paper is to call for multidisciplinary research for scientists with various backgrounds (e.g. robotics, computer scientists, mechanical and electrical engineers) to sit together to find the solutions to the existing security problems. For instance, recent births of domestic and hospital robots have significantly boosted up the importance of cybersecurity, relatively new research areas that people in the robotics community did not have to face before.

We envisage that in the future the trend will be shifted towards the use of computational intelligence approach rather than traditional model-based technique, whose performance is reliant on the accuracy of the assumed mathematical model of the systems. We will also witness more applications of the cyber-physical systems, specifically designed for trusted operations of robotic and industrial automation platforms.

## REFERENCES

- [1] S. Parkinson, P. Ward, K. Wilson, and J. Miller. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transport Systems*, 18(11):2898–2915, November 2017.
- [2] H. G. Garakani, B. Moshiri, and S. Safavi-Naeini. Cyber security challenges in autonomous vehicle: Their impact on rf sensor and wireless technologies. In *18th International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM)*, Waterloo, ON, Canada, August 2018. IEEE.
- [3] Z. Song, A. Skuric, and K. Ji. A recursive watermark method for hard real-time industrial control system cyber-resilience enhancement. *IEEE Transactions on Automation Science and Engineering*, pages 1–14, 2020.

- [4] M. Leccadito, T. Bakker, R. Klenke, and C. Elks. A survey on securing uas cyber physical systems. *IEEE Aerospace and Electronic Systems Magazine*, 33(10):22–32, November 2018.
- [5] Y. Tian, J. Guo, Y. Wu, and H. Lin. Towards attack and defense views of rational delegation of computation. *IEEE Access*, 7:44037–44049, March 2019.
- [6] F. Ahmadloo and F. R. Salmasi. A cyber-attack on communication link in distributed systems and detection scheme based on h-infinity filtering. In *IEEE International Conference on Industrial Technology (ICIT)*, pages 698–703. IEEE, 2017.
- [7] I. Abeykoon and X. Feng. A forensic investigation of the robot operating system. In *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 851–857. IEEE, 2017.
- [8] X. Jin, W. M. Haddad, and T. Yucelen. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. *IEEE Transactions on Automatic Control*, 62(11):6058–6064, 2017.
- [9] F. Santoso. A new framework for rapid wireless tracking verifications based on optimized trajectories in received signal strength measurements. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 45(11):1424–1436, November 2015.
- [10] F. Yao abd L. Jia. A collaborative multi-agent reinforcement learning anti-jamming algorithm in wireless networks. *IEEE Wireless Communications Letters*, 8(4):1024–1027, August 2019.
- [11] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick. Highly efficient known-plaintext attacks against orthogonal blinding based physical layer security. *IEEE Wireless Communications Letters*, 4(1):34–37, October 2015.
- [12] B. Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass, and P. Schartner. Security for the robot operating system. *Robotics and Autonomous Systems*, 98:192–203, 2017.
- [13] F. Santoso, M. A. Garratt, S. G. Anavatti, and I. Petersen. Robust hybrid nonlinear control systems for the dynamics of a quadcopter drone. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, June 2018.
- [14] Z. Li, Y. Xia, C. Su, J. Deng, J. Fu, and W. He. Missile guidance law based on robust model predictive control using neural-network optimization. *IEEE Transactions on Neural Networks and Learning Systems*, 26(8):1803–1809, August 2015.
- [15] J. Cervantes, W. Yu, S. Salazar, and I. Chairez. Takagi–sugeno dynamic neuro-fuzzy controller of uncertain nonlinear systems. *IEEE Transactions on Fuzzy Systems*, 25(6):1601–1615, December 2017.
- [16] W. Qi, W. Cai, Q. Ji, and Y. Cheng. A design of nonlinear adaptive pid controller based on genetic algorithm. In *Chinese Control Conference*, pages 175–178, 2006.
- [17] L. Liu, D. Wang, Z. Peng, C. L. P. Chen, and T. Li. Bounded neural network control for target tracking of underactuated autonomous surface vehicles in the presence of uncertain target dynamics. *IEEE Transactions on Neural Networks and Learning Systems*, 30(4):1241–1249, September 2019.
- [18] W. J. Han and I. S. Han. Bio-inspired computing of vision — fuzzy and neuromorphic processing. In *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE 2011)*, pages 747–750, Taipei, Taiwan, June 2011. IEEE.
- [19] P. Melin. *Type-2 Fuzzy Logic and Systems: Studies in Fuzziness and Soft Computing*, chapter Type-2 Fuzzy Logic in Pattern Recognition Applications, pages 89–104. Springer, 2018.
- [20] O. Linda, M. Manic, T. Vollmer, and J. Wright. Fuzzy logic based anomaly detection for embedded network security cyber sensor. In *IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, pages 1–8. IEEE, 2011.
- [21] O. Linda, M. Manic, J. Alves-Foss, and T. Vollmer. Towards resilient critical infrastructures: application of type-2 fuzzy logic in embedded network security cyber sensor. In *4th International Symposium on Resilient Control Systems*, pages 26–32. IEEE, 2011.
- [22] M Alazab and M. J. Tang, editors. *Deep Learning Applications for Cyber Security*. Springer, 2019.
- [23] Z. Bankovica, D. Stepanovic, S. Bojanica, and O. Nieto-Taladriza. Improving network security using genetic algorithm approach. *Computers & Electrical Engineering*, 33:438–450, 2007.
- [24] Y. Ashibani and Q. H. Mahmoud. Cyber physical systems security: Analysis, challenges and solutions. *Computers and Security*, 68:81–97, April 2017.

- [25] A. Humayed, J. Lin, F. Li, and B. Luo. Cyber-physical systems security—a survey. *IEEE Internet of Things Journal*, 4:1802–1830, December 2017.
- [26] M. Wolf and D. Serpanos. Safety and security in cyber-physical systems and internet-of-things systems. *Proceedings of the IEEE*, 106:9–20, January 2018.
- [27] D. Ding, Q. L. Han, X. Ge, and J. Wang. Secure state estimation and control of cyber-physical systems: A survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51:176–190, January 2021.
- [28] F. Santoso, M. A. Garratt, S. G. Anavatti, O. Hasanein, and T. Stenhouse. Entropy fuzzy system identification for the heavy flight dynamics of a model-scale helicopter. *IEEE/ASME Transactions on Mechatronics*, pages 1–12, December 2019.
- [29] F. Santoso, M. A. Garratt, S. G. Anavatti, M. Ferdous, J. Wang, and P. V. Tran. *Unmanned Aerial Systems: Theoretical Foundation and Applications*, chapter Evolutionary Aerial Robotics: The Human Way of Learning. Springer Berlin Heidelberg, Germany, 2020.
- [30] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava. Analyzing the cyber-physical impact of cyber events on the power grid. *IEEE Transactions on Smart Grid*, 6(5):2444 – 2453, September 2015.
- [31] O. Hassanein, S. G. Anavatti, and T. Ray. Fuzzy modeling and control for autonomous underwater vehicle. In *Proceedings of the 5th International Conference on Automation, Robotics and Applications*, pages 169–174, Wellington, New Zealand, December 2011. IEEE.
- [32] F. Santoso, M. A. Garratt, and S. G. Anavatti. Hybrid PD-fuzzy and PD controllers for trajectory tracking of a quadrotor unmanned aerial vehicle: Autopilot designs and real-time flight tests. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pages 1–12, April 2019.
- [33] F. Santoso, M. A. Garratt, M. R. Pickering, and Md. Asikuzzaman. 3D mapping for visualization of rigid structures: A review and comparative study. *IEEE Sensors*, 16:1484–1507, March 2015.
- [34] B. Gerkey. Why ROS 2? <https://design.ros2.org/>, 2017.
- [35] L. do O, P. A. Prates, R. Mendonca, A. Lourenco, F. Marques, and J. Barata. Autonomous 3-D aerial navigation system for precision agriculture. In *IEEE 28th International Symposium on Industrial Electronics (ISIE)*, pages 1144–1149., Vancouver, BC, Canada, June 2019. IEEE.
- [36] Z. Sen, S. Lei, C. Zhongliang, Z. Lishuang, and L. Jingtai. A ROS-based smooth motion planning scheme for a home service robot. In *34th Chinese Control Conference (CCC)*, pages 5119–5124, Hangzhou, July 2015. IEEE.
- [37] National Aeronautics and Space Administration (NASA). R2 robonaut. <https://robonaut.jsc.nasa.gov/R2/>, 2019.
- [38] ECA Group. Cyber security for unmanned systems. <https://www.ecagroup.com/en/cyber-security-unmanned-systems>, 2020.
- [39] B. Dieber, R. White, S. TAurer, B. Breiling, G. Caiazza, H. Chrsitensen, and A. Cortesi. *Studies in Computational Intelligence Robot Operating System*, volume 4, chapter Penetration Testing ROS, pages 183–225. Springer, 2020.
- [40] R. C. White and H. M. Quigley. SROS: Securing ROS over the wire, in the graph, and through kernal. In *Humanoids 2016: Toward Humanoid Robots*, 2016.
- [41] Open Source Robotics Foundation. *Secure Robot Operating System*. USA, 2016.
- [42] *TARDEC 30 year strategy value stream analysis*, 2017.
- [43] H. Zhu, M. L. Cummings, M. Elfar, Z. Wang, and M. Pajic. Operator strategy model development in UAV hacking detection. *IEEE Transactions on Human-Machine Systems*, 49(6):540–549, December 2019.
- [44] J. Gaspar, R. Ferreira, and P. Sebastião amd N. Souto. Capture of UAVs through gps spoofing. In *Global Wireless Summit (GWS)*, pages 21–26, Thailand, November 2018. IEEE.
- [45] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, Joerger M, and B. Pervan. Gps spoofing detection using raim with ins coupling. In *IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, pages 1232–1239, Monterey, CA, USA, May 2014. IEEE.
- [46] N. I. Ziedan. Investigating and utilizing the limitations of spoofing in a map-matching anti-spoofing algorithm. In *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014)*, pages 2843–2852., Tampa, Florida, September 2014. IEEE.
- [47] S. Furnell. *Handbook of Internet Crime*, chapter Hackers, viruses, and malicious software, pages 173–451. Taylor and Francis Group, NY, USA, 2010.
- [48] H. Lee, S. Eom, J. Park, and I. Lee. UAV-aided secure communications with cooperative jamming. *IEEE Transactions on Vehicular Technology*, 67(10):9385–9392, October 2018.
- [49] C Popper, M Strasser, and S Capkun. Anti-jamming broadcast communication using uncoordinated spread spectrum techniques. *IEEE Journal on Selected Areas in Communications*, 28(5):703–715, May 2010.
- [50] K. Hartmann and O. V. Guericke. UAV exploitation: A new domain for cyber power. In *8th International Conference on Cyber Conflict*. NATO CCD COE Publications, 2016.
- [51] J. A. Steinmann, R. F. Babiceanu, and R. Seker. UAS security: Encryption key negotiation for partitioned data. In *Integrated Communications Navigation and Surveillance (ICNS)*, pages 1E4–1–1E4–7, Herndon, VA, USA, April 2016. IEEE.
- [52] S. W. Kim. Physical integrity check in cooperative relay communications. *IEEE Transactions on Wireless Communications*, 14(11):6401–6413, November 2015.
- [53] L. Liu, Y. Lu, and C. Y. Suen. Variable-length signature for near-duplicate image matching. *IEEE Transactions on Image Processing*, 24(4):1282–1296, April 2015.
- [54] M. Uddin, S. Islam, and A. Al-Nemrat. A dynamic access control model using authorising workflow and task-role-based access control. *IEEE Access*, 7:166676 –166689, October 2019.
- [55] J. M. Hamamreh, H. M. Furqan, and H. Arslan. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communication Surveys and Tutorials*, 21(2):1773–1828, October 2019.
- [56] Y. Zhi, G. Xiantai, J. Weidong, X. Haowen, and Z. Lingyuan. Reverse engineering for UAV control protocol based on detection data. In *2nd International Conference on Multimedia and Image Processing (ICMIP)*, pages 301–304, China, March 2017. IEEE.
- [57] B. F. Mary and D.I. G. Amalarethnam. Data security enhancement in public cloud storage using data obfuscation and steganography. In *World Congress on Computing and Communication Technologies (WCCCT)*, pages 181–184, India, February 2017. IEEE.
- [58] H. Cheng D. Wang, D. He and P. Wang. fuzzypsrm: A new password strength meter using fuzzy probabilistic context-free grammars. In *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 595–606. IEEE, 2016.
- [59] Joost N Kok, Egbert J Boers, Walter A Kusters, Peter Van der Putten, and Mannes Poel. Artificial intelligence: definition, trends, techniques, and cases. *Artificial intelligence*, 1:270–299, 2009.
- [60] Jafar Alzubi, Anand Nayyar, and Akshi Kumar. Machine learning from theory to algorithms: An overview. *Journal of Physics: Conference Series*, 1142(1):012012, nov 2018.
- [61] S. Morante, JG Victores, and C Balaguer. Cryptobotics: Why robot need cyber safety. *Front Robot and AI*, 2(23):1–4, September 2015.
- [62] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *IEEE Conference on Technologies for Homeland Security (HST)*, pages 585–590, Waltham, MA, 2012. IEEE.
- [63] G. S Lee and B. Thuraisingham. Cyberphysical systems security applied to telesurgical robotics. *Computer Standards & Interfaces*, 34:225–229, 2011.
- [64] H. H. King, K. Tadano, R. Donlin, D. Friedman, M. J.H. Lum, V. Asch, C. Wang, K. Kawashima, and B. Hannaford. Preliminary protocol for interoperable telesurgery. In *International Conference on Advanced Robotics*, Munich, Germany, 2009. IEEE.
- [65] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, and H. J. Chizeck. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. *arXiv*, May 2015.
- [66] M. Hans, B. Graf, and R.D. Schraft. Robotic home assistant care-o-bot: past-present-future. In *Proceedings of the 11th IEEE International Workshop on Robot and Human Interactive Communication*, pages 380–385, Berlin, Germany, September 2002. IEEE.
- [67] B. Graf, A. Hans, J. Kubacki, and R.D. Schraft. Robotic home assistant care-o-bot ii. In *Robotic home assistant Care-O-bot II*, pages 2343–2344, Houston, TX, USA., October 2002. IEEE.
- [68] Y. Iwano, K. Osuka, and H. Amano. Experimental study of traction robot system for rescue against nuclear disaster. In *IEEE International Safety, Security and Rescue Robotics*, pages 93–98, Kobe, Japan, June 2005. IEEE.
- [69] E Pan, D. Guan, W. Xu, and B. Hu. Control system of a small intelligent inspection robot for nuclear power plant use. In *IEEE International Conference on Information and Automation*, pages 837–842, Lijiang, China, August 2015. IEEE.



- [70] N. Takase, J. Botzheim, and N. Kubota. Robot edutainment on walking motion of multi-legged robot. In *Second International Conference on Robot, Vision and Signal Processing*, pages 229–233, Kitakyushu, Japan, December 2013. IEEE.
- [71] I-W Park, J.-Y Kim, and J.-H Oh. Online biped walking pattern generation for humanoid robot khr-3(kaist humanoid robot - 3: Hubo). In *6th IEEE-RAS International Conference on Humanoid Robots*, pages 398–403, Genova, Italy, February 2006. IEEE.
- [72] A. Sen and S. Madria. Risk assessment in a sensor cloud framework using attack graphs. *IEEE Transactions on Services Computing*, 10(6):942 – 955, November 2017.
- [73] S. Musman and A. Temin. A cyber mission impact assessment tool. In *IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, USA, April 2015. IEEE.
- [74] D. Ding, Q.-L. Han, Z. Wang, and X. Ge. A survey on model-based distributed control and filtering for industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 15(5):2483–2499, March 2019.
- [75] K. Manandhar, X. Cao, F. Hu, and Y. Liu. Detection of faults and attacks including false data injection attack in smart grid using kalman filter. *IEEE Transactions on control of network systems*, 1(4):370–379, December 2014.
- [76] F. Santoso and R. Malaney. Tracking-based wireless intrusion detection for vehicular networks. In *IEEE Vehicular Technology Conference (VTC Fall)*. IEEE, September 2011.
- [77] Y. Liu, H. Xin, Z. Qu, and D. Gan. An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks. *IEEE Transactions on Smart Grid*, 7(6):2923–2932, November 2016.
- [78] F. Santoso, M. A. Garratt, and S. G. Anavatti. T2-ETS-IE: Type-2 evolutionary takagi-sugeno fuzzy inference systems with information entropy-based pruning technique. *IEEE Transactions on Fuzzy Systems*, 28(10):2665–2672, October 2020.
- [79] N. N. Karnik, J. M. Mendel, and Q. Liang. Type-2 fuzzy logic systems. *IEEE Transactions on Fuzzy Systems*, 7(6):643–658, December 1999.
- [80] L. An and G.-H. Yang. Dexentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems againsts intermittent dos attacks. *IEEE Transactions on Cybernetics*, 49(3):827–838, March 2019.
- [81] B. A. Tama, M. Comuzzi, and K.-H. Rhee. TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. *IEEE Access*, 7:94497–94507, July 2019.
- [82] M. Tavallae, E. Bagheri, W. Lu, and A. A. Ghorbani. A detailed analysis of the KDD CUP 99 data set. In *2nd IEEE Symp. Comput. Intell. Secure Defence Appl.*, pages 1–6, July 2009.
- [83] N. Moustafa and J. Slay. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, pages 1–6, November 2015.
- [84] A. H. Almutairi and N. T. Abdelmajeed. Innovative signature based intrusion detection system: Parallel processing and minimized database. In *International Conference on the Frontiers and Advances in Data Science (FADS)*, pages 114–119, Xian, 2017.
- [85] K. Hwang, M. Cai, Y. Chen, and M. Qin. Hybrid intrusion detection with weighted signature generation over anomalous internet episodes. *IEEE Transactions on Dependable and Secure Computing*, 4(1):41–55, January 2007.
- [86] M. Roesch. SNORT—lightweight intrusion detection for networks. In *Proc. USENIX 13th Systems Administration Conf. (LISA '99)*, pages 229–238, 1999.
- [87] A. R. Baker, B. Caswell, M. Poor, S. Northcutt, R. Alder, J. Babbin, J. Beale, A. Doxtater, J. C. Foster, T. Kohlenberg, and M. Rash. *Snort 2.1 Intrusion Detection*. Syngress, 2004.
- [88] V. Paxson. Bro: A system for detecting network intrusions in real time. In *Proc. Seventh USENIX Security Symp*, 1998.
- [89] S. Siddiqui, M. S. Khan, and K. Ferens. Multiscale hebbian neural network for cyber threat detection. In *International Joint Conference on Neural Networks (IJCNN)*, pages 1427–1434, Anchorage, AK, 2017.
- [90] F. Farivar, M. S. Haghghi, Al. Jolfaei, and M. Alazab. Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT. *IEEE Transactions on Industrial Informatics*, 16(4):2716–2725, April 2020.
- [91] S. Potluri, C. Diedrich, G. Kumar, and R. Sangala. Identifying false data injection attacks in industrial control systems using artificial neural networks. In *22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8, Limassol, Cyprus, 2017. IEEE.
- [92] E. A. Newcomb and R. Hammell. FLUF: Fuzzy logic utility framework to support computer network defense decision making. In *Annual Conference of the North American Fuzzy Information Processing Society (NAFIPS)*, pages 1–6, El Paso, TX, 2016. IEEE.
- [93] F. Martinelli, F. Mercaldo, V. Nardone, and A. Santone. Car hacking identification through fuzzy logic algorithms. In *IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, Naples, Italy, July 2017. IEEE.
- [94] D. Wijayasekara, O. Linda, M. Manic, and C. Rieger. FN-DFE: Fuzzy-neural data fusion engine for enhanced resilient state-awareness of hybrid energy systems. *IEEE Transactions on Cybernetics*, 44(11):2065–2075, November 2014.
- [95] O.S. Amosov, Y.S. Ivanov, and S. G. Amosova. Recognition of abnormal traffic using deep neural networks and fuzzy logic. In *International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*. IEEE, October 2019.
- [96] W. Li, W. Meng, C. SU, and L. F. Kwok. Towards false alarm reduction using fuzzy if-then rules for medical cyber physical systems. *IEEE Access*, 6:6530–6539, January 2018.
- [97] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Hans. Enhanced network anomaly detection based on deep neural networks. *IEEE Access*, 6:48231–48246, July 2018.
- [98] A. Giuseppi, A. Tortorelli, R. Germana, F. Liberati, and A. Fiaschetti. Securing cyber-physical systems: an optimization framework based on OSSTMM and genetic algorithms. In *27th Mediterranean Conference on Control and Automation (MED)*, pages 50–56, Israel, July 2019. IEEE.
- [99] D. Zhang, H. Song, and L. Yu. Robust fuzzy-model-based filtering for nonlinear cyber-physical systems with multiple stochastic incomplete measurements. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 47(8):1826–1838, June 2016.
- [100] F. Santoso and A. Finn. Trusted operations of a military ground robot in the face of man-in-the-middle cyberattacks using deep learning convolutional neural networks: Real-time experimental outcomes. *IEEE Transactions on Dependable and Secure Computing*.
- [101] A. N. Jahromi, H. Karimipour, A. Dehghantaha, and K. K. R. Choo. Toward detection and attribution of cyber-attacks in iot-enabled cyber-physical systems. *IEEE Internet of Things Journal*, 8(17):13712–13722, 2021.
- [102] S. Rahman, M. Ahmed, and M. S. Kaiser. NFIS based cyber physical attack detection system. In *5th International Conference on Informatics, Electronics and Vision (ICIEV)*, pages 944–948, Bangladesh, 2016. IEEE.
- [103] Z. Bankovic, D. Stepanovic, S. Bojanica, and O. Nieto-Taladriza. Improving network security using genetic algorithm approach. *Computers & Electrical Engineering*, 55(5–6):438–451, July 2007.
- [104] S. Misra, S. Goswami, and C. Taneja. Multivariate data fusion-based learning of video content and service distribution for cyber physical social systems. *IEEE Transactions on Computational Social Systems*, 3(1):1–12, May 2016.
- [105] F. Santoso and A. Finn. A data-driven cyber-physical system using deep-learning convolutional neural networks: Study on false-data injection attacks in an unmanned ground vehicle under fault-tolerant conditions. *IEEE Transactions on Systems, Man, and Cybernetics*, 53(1):346–356, January 2023.
- [106] L. Liu, B. Wang, C. Deng, M. Zhu, S. Yin, and S. Wei. Anole: A highly efficient dynamically reconfigurable crypto-processor for symmetric-key algorithms. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(12):3081–3094, December 2018.
- [107] M. Malik, M. Dutta, and J. Granjal. A survey of key bootstrapping protocols based on public key cryptography in the internet of things. *IEEE Access*, pages 27443–27464, February 2019.
- [108] F. Guo, W. Susilo, and Y. Mu. Distance-based encryption: How to embed fuzziness in biometric-based encryption. *Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption*, 11(2):247–257, October 2015.
- [109] N. R. Prasad P. N. Mahalle, P. A. Thakre and R. Prasad. A fuzzy approach to trust based access control in internet of things. In *Wireless VITAE 2013*, pages 1–5. IEEE, 2013.
- [110] Q. Zhang, C. Zhou, Y.-C. Tian, N. Xiong, Y. Qin, and B. Hu. A fuzzy probability bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. *IEEE Transactions on Industrial Informatics*, 14(6):2497–2506, June 2018.
- [111] Y. Shi, R. Eberhart, and Y. Chen. Implementation of evolutionary fuzzy systems. *IEEE Trans. Fuzzy System*, 7(2):109–119, 1999.
- [112] S. N. Narayanan, A. Joshi, and R. Bose. Abate: Automatic behavioral abstraction technique to detect anomalies in smart cyber-physical

- systems.. *IEEE Transactions on Dependable and Secure Computing*, 19(3):1673–1686, May-June 2022.
- [113] F. Mercaldo G. Ciaramella, F. Martinelli and A. Santone. Exploring quantum machine learning for explainable malware detection. In *International Joint Conference on Neural Networks (IJCNN)*, pages 1–6. IEEE, 2023.
- [114] Wei-Chi Ku. Weaknesses and drawbacks of a password authentication scheme using neural networks for multiserver architecture. *IEEE Transactions on Neural Networks*, 16(4):1002–1005, July 2025.
- [115] J. Vieira, F. M. Dias, and A. Mota. Neuro-fuzzy systems: A survey. In *Proceedings of the 4th WSEAS International Conference on Neural Networks*, pages 1–6. IEEE, 2004.
- [116] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, and J. Chen. Threshold-free physical layer authentication based on machine learning for industrial wireless CPS. *IEEE Transactions on Industrial Informatics*, 15(12):6481–6491, December 2019.
- [117] J. Ning, Y. Wang, J. Yang, H. Gacanin, and S.Ci. A novel malware traffic classification method using semi-supervised learning. In *Proceedings of the IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, pages 1–5, Norman, OK, US, December 2021. IEEE.
- [118] Y. Gao, Y. Liu, Y. Jin, J. Chen, and H. Wu. A novel semi-supervised learning approach for network intrusion detection on cloud-based robotic system. *IEEE Access*, 6:50927–50938, 2018.
- [119] D. A. M. Villalba, D. F. M. Varon, F. G. Pórtela, and O. A. D. Triana. Intrusion detection system (ids) with anomaly-based detection and deep learning application. In *V Congreso Internacional en Inteligencia Ambiental, Ingeniería de Software y Salud Electrónica y Móvil (AmITIC)*, pages 1–4, 2022.
- [120] S. Ahmed, Y. Lee, S. Hyun, and I. Koo. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Transactions on Information Forensics and Security*, 14(10):2765–2777, October 2019.
- [121] T. Zoppi, A. Ceccarelli, and A. Bondavalli. Into the unknown: Unsupervised machine learning algorithms for anomaly-based intrusion detection. In *50th Annual-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*, pages 81–81, 2020.
- [122] H. Narasimhan, V. Ravi, and N. Mohammad. Unsupervised deep learning approach for in-vehicle intrusion detection system. *IEEE Consumer Electronics Magazine*, 12(1):103–108, 2023.
- [123] L. Shahbandayeva, U. Mammadzada, I. Manafova, S. Jafarli, and A. Z. Adamov. Network intrusion detection using supervised and unsupervised machine learning. In *2022 IEEE 16th International Conference on Application of Information and Communication Technologies (AICT)*, pages 1–7, 2022.
- [124] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang. Online cyber-attack detection in smart grid: A reinforcement learning approach. *Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach*, 10(5):5174–5185, September 2019.
- [125] C. Hu, J. Yan, and X. Liu. Reinforcement learning-based adaptive feature boosting for smart grid intrusion detection. *IEEE Transactions on Smart Grid*, 14:3150–3163, 2023.
- [126] J. Nyberg, P. Johnson, and A. Méhes. Cyber threat response using reinforcement learning in graph-based attack simulations. In *Proceedings of IEEE/IFIP Network Operations and Management Symposium*, pages 1–4, Budapest, 2022. IEEE.
- [127] T. V. Phan and T. Bauschert. Deepair: Deep reinforcement learning for adaptive intrusion response in software-defined networks. *IEEE Transactions on Network and Service Management*, 19:2207–2218, September 2022.
- [128] A. L. Buczak and E. Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys and Tutorials*, 18:1153–1176, second quarter 2016.
- [129] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath. Generative adversarial networks: An overview. *IEEE Signal Processing Magazine*, 35(1):53–65, 2018.
- [130] J. H Holland. Genetic algorithms. *Scientific American*, 1:66–73, July 1992.
- [131] Fu Rui, Mohammed Abdulhakim Al-Absi, Ki-Hwan Kim, Ahmed Abdulhakim Al-Absi, and Hoon Jae Lee. Genetic algorithm for decrypting user’s personal information. In Prasant Kumar Pattnaik, Mangal Sain, Ahmed A. Al-Absi, and Pardeep Kumar, editors, *Proceedings of International Conference on Smart Computing and Cyber Security*, pages 197–204, Singapore, 2021. Springer Singapore.
- [132] S. E. Benaicha, L. Saoudi, S. E. B. Guermèche, and O. Lounis. Intrusion detection system using genetic algorithm. In *2014 Science and Information Conference*, pages 564–568, London, 2014.
- [133] H. A. Sukhni, M. A. Al-Khasawneh, and F. H. Yusoff. A systematic analysis for botnet detection using genetic algorithm. In *2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, pages 63–66, Malaysia, 2021. IEEE.
- [134] C. Lecerf. Tackling the stability/plasticity dilemma with double loop dynamic systems. In *Proceeding of the European Symposium of Artificial Neural Networks*, pages 153–158. IEEE, April 1999.
- [135] F. Santoso, M. A. Garratt, and S. G. Anavatti. State-of-the-art intelligent flight control systems in unmanned aerial vehicles. *IEEE Transactions on Automation Science and Engineering*, 15(2):613–627, February 2018.
- [136] M. Mermillod, A. Bugajska, and P. Bonin. The stability-plasticity dilemma: investigating the continuum from catastrophic forgetting to age-limited learning effects. *Frontiers in Psychology*, 504:1–3, August 2013.



**Fendy Santoso** received the master’s degree in Electrical and Computer Systems Engineering from Monash University, Melbourne, VIC, Australia, in 2007, and the Ph.D. degree in Electrical Engineering from The University of New South Wales, Sydney, NSW 2052, Australia, in 2012. As a Senior Research Fellow and Senior Lecturer in the Artificial Intelligence and Cyber Futures (AICF) Institute, Charles Sturt University, Bathurst NSW 2795 Australia, Fendy currently leads a research program under the Defence and cybersecurity theme. Fendy was a Research Fellow with the Defense and Systems Institute, UniSA STEM, The University of South Australia, Mawson Lakes, SA 5095, Australia, and also with the Autonomous Systems Laboratory, School of Engineering and Information Technology, UNSW Canberra, Campbell, ACT 2612, Australia, where he also currently holds a visiting research fellowship position.

His current research interests include control systems and artificial intelligence with applications in robotics and cybersecurity. Fendy was the recipient of the “Distinguished Early Career Travel Fellowship” (under the Vice Chancellor’s Fellowship) Award from the University of Wollongong, Wollongong NSW 2522, Australia. He has successfully made some remarkable contributions to intelligent robotics by innovating the concept of bio-mimetic self-learning by means of evolving fuzzy systems.



**Anthony Finn** graduated from Cambridge University with a Ph.D. in 1989. He is a Professor of Autonomous Systems at the University of South Australia and was Director of the Defense and Systems Institute (DASI) from 2011–2019. He has published two books and around two hundred book chapters, journal articles, refereed conference papers, and research reports. Before joining DASI in 2010, Professor Finn worked at Australia’s Defense Science and Technology Organization (DSTO) for almost twenty years, the last ten of which were spent leading a team of around forty scientists and engineers conducting research into the defense applications of autonomous and unmanned vehicles. Professor Finn worked as a research consultant for several large organizations in Europe.