Securing Vehicle-to-Grid Networks: A Bio-Inspired Intrusion Detection System

Kheireddine Mekkaoui [*,a], Mansour Mekour[b], and Hamza Teggar[c]

[a] Department of computer sciences, University of Saida - Dr Moulay Tahar, 20000, Algeria.
Email: Kheireddine.mekkaoui@univ-saida.dz, Tel: +213 550 497 966

[b] Department of computer sciences, University of Saida - Dr Moulay Tahar, 20000, Algeria.
Email: mansour.mekour@univ-saida.dz, Tel: +213 671 898 560

[c] Department of computer sciences, University of Mascara - Dr Moulay Tahar, 29000, Algeria.
Email: Hamza.tegar@univ-mascara.dz ,Tel: +213 770 364 342

[*] Corresponding author: Kheireddine.mekkaoui@univ-saida.dz

Abstract

The Vehicle-to-Grid (V2G) network enables electric vehicles (EV) to connect and exchange both energy and data with the Smart Grid (SG), thus ensuring bidirectional communication and contributing to environmental protection. However, the V2G network faces various security challenges, including data integrity, the security of electrical systems, physical protection of charging systems, data confidentiality, and system interoperability. Therefore, it is crucial to implement appropriate security mechanisms.This paper proposes a bio-inspired intrusion detection system (IDS) based on machine learning to predict and mitigate attacks on V2G network. The objective of this work is to enhance the security of V2G networks by providing solutions against Man-in-the-Middle (MitM) and Denial of Service (DoS) attacks. Simulations conducted using the MiniV2G simulator show that the proposed IDS achieves a detection accuracy of 98.93%, thereby improving the reliability of the V2G network for users and offering better protection for electric vehicle charging stations against DoS and MitM attacks.

KEYWORDS: V2G, Smart grid, ISO 15118, V2G security, IDS, attack prediction, Grouping Cockroaches Classifier (GCC), MitM attack, DoS attack.

1. Introduction

Today, humanity is facing numerous climate challenges that impact the planet. It is essential to take urgent measures to protect the Earth and preserve the environment with minimal pollution levels, in the hope of reducing climate changes. According to [1-2], this phenomenon is directly linked to the industrial development we are experiencing today, as it significantly contributes to the pollution of our planet.

The automotive industry is not exempted, with the manufacturing of fuel vehicles (gasoline, diesel) emitting a considerable amount of carbon dioxide (CO2), contributing to environmental pollution [3]. In this context, the automotive industry is working on the transition from fuel vehicles to EVs to contribute to planet protection. This transition involves prerequisites such as implementing standards capable of regulating this increasingly growing technology [4]. Indeed, according to a study by Canalys [5], electric vehicle sales experienced exponential growth in 2023, and it is estimated that by 2030, electric vehicles (EVs) will represent nearly 50% of sales car in the worldwide, as shown in Figure 1 .

EVs require energy to operate. They must be connected to the electrical grid through public or residential charging stations in order to charge and discharge their batteries; this interconnection process is called Vehicle-to-Grid (V2G). V2G is part of the SG, responsible of bidirectional exchanges between a EV and its charging station (EVCS) [6-8].

Communication among the various components of a V2G network, as depicted in Figure 2, involves the EV, the EVCS, and the Smart Grid (SG). These communication are conducted using the ISO/IEC 15118 protocol, established by the International Organization for Standardization (ISO) [9].

The norme ISO 15118 defines bidirectional communication protocols for EV charging. It describes the interactions between EVs, EVCS, and the network infrastructure necessary for the charging process. This standard covers technical aspects of communication, such as communication protocols, security management, management data, and compatibility between different systems. It is a key tool to guarantee the interoperability of the V2G system for efficient and secure use, in the case of recharging vehicle batteries or the use of the energy stored in these batteries during peak hours in order to optimize the electricity consumption by customers [10-11].

However, it should be noted that ISO 15118, despite being a reference for V2G security, does not address all security aspects. It does not provide specific guidance on all solutions and methods to implement for V2G protection [12-15]. The limitations of this standard have been left to researchers, who have proposed several solutions to enhance security. Intrusion Detection Systems (IDS) are considered one of the most promising solutions to protect V2G networks [16].

During this decade, the Internet and computer systems, including V2G networks, have experienced exponential growth in security issues. Indeed, several studies have shown a significant increase in intrusions and attacks in recent years [17-18]. In this context, the V2G network is not immune from these security threats.

Cyber-attacks against the V2G process can take various forms, targeting different aspects of the system's operations. Here are some common types of cyber-attacks that can alter the functioning of V2G networks [19-20]:

- DoS Attack: A Denial of Service attack aims to make a service or network unavailable by inonding the target with excessive traffic. Attackers often use botnets to generate a massive flow of requests or data in order to saturate resources and prevent legitimate users from accessing the service. In V2G network, this attack can paralyze charging stations and disrupt communications between EVs and the SG, leading to service interruptions, challenges in energy demand management, and financial losses due to service unavailability.

- MitM Attack : A man-in-the-middle attack occurs when an attacker intercepts and potentially alters communications between two parties without their knowledge. The attacker can thus eavesdrop on exchanged data or inject false information. This type of attack alter the confidentiality and the integrity of the data exchanged between EVs and the SG. It can provoke incorrect energy management decisions, theft of sensitive data, and unauthorized actions that disrupt network balance.

- Malware Attack: This attack involves the insertion of malicious codes into the V2G network system. These programs can perform various dangerous activities such as data theft, operational disruption, or unauthorized control of devices. The presence of malware, in V2G networks, can lead to leaks of sensitive data, system malfunctions, and loss of control over critical infrastructure, compromising the security and reliability of the network.

- Data Integrity Attack: This attack provoke the unauthorized modification of information being transmitted or stored within the V2G network. Attackers aim to alter data to alter decisions or cause operational errors. Such attacks can lead to incorrect energy management decisions, financial losses due to erroneous transactions, and degradation of user trust in the system, affecting the overall operational efficiency of the network.

- Eavesdropping (Passive Attack): An eavesdropping attack involves a passive capture of communications within the V2G network by attackers who first seek to access sensitive information without altering the data. Tampering with privacy can lead to sensitive information such as invoice details and transaction data being leaked, thereby facilitating subsequent attacks and affecting user privacy.

- Spoofing Attack: This attack occurs when an attacker impersonates a device or user within the V2G network for the purpose of gaining unauthorized access or performing unauthorized actions. The consequences of such an attack include unauthorized access to network resources, non-legitimate transactions and potentially illicit control of energy flows, thus disrupting the normal and secure operation of the network.

- Replay Attacks: This attack involves capturing and reusing legitimate communications in order to disrupt the network. Attackers retransmit valid messages to create unauthorized actions or disruptions. In V2G networks, these attacks can cause duplication of legitimate instructions, disrupting network synchronization and coordination, leading to energy imbalances and operational errors.

- Sybil Attack : A Sybil attack occurs when an attacker creates multiple false identities to dominate or manipulate the network. The presence of many false identities, in a network, can affect the network's decision-making mechanisms, leading to manipulated actions, and erroneous data analysis and disrupted operations.

- Physical Attack: This type of attack involves unauthorized direct access to V2G infrastructure, such as charging stations or control units, often to inject or implant malicious devices. Consequences include physical damage, service interruptions, and the potential insertion of malicious access points that can be exploited for further cyberattacks.

- Side-Channel Attack: A side-channel attack exploits indirect information, such as electromagnetic leaks or power consumption patterns, to extract sensitive data without directly interfering with communications. The impact of this attack on V2G Network is such attacks can reveal cryptographic keys or other critical information, compromising the security of communications and transactions within the network.

- Firmware and Software Exploitation: This attack exploits vulnerabilities in the firmware or software of V2G components to gain unauthorized access or take control of the system. Exploiting these vulnerabilities can allow complete system takeover, unauthorized data

modifications, and service interruptions, endangering the security and integrity of the network.

- Insider Attack: An insider attack is carried out by someone with legitimate access to the V2G network who uses their privileges to carry out malicious activities such as data theft or system crash. Insider attacks can lead to privacy breaches, direct alteration and destruction of user trust.

Each of these attack types poses significant risks to the V2G process, potentially affecting the stability, security, and reliability of the grid and the connected vehicles. Effective detection and mitigation strategies are essential to protect the network against these threats.

Among all these attacks, this study focus on DoS and MitM attacks in V2G networks. Indeed, the concentration on these types of attacks is based on their critical impact and prevalence, as well as the specific vulnerabilities they exploit within V2G systems. Below, we outline the key reasons for our focus:

- Prevalence and Impact of DoS Attacks : DoS attacks pose a significant threat to the availability and reliability of V2G networks. According to recent studies, DoS attacks account for over 60% of all attacks targeting electric vehicle charging infrastructures in V2G networks [21-22]. Indeed, according to [23], during the fourth quarter of 2023, a 770% increase in DoS attacks on the network layer was observed compared to the previous year. Figure 3 represents the significant increase in DoS attacks over last 5 years.

These attacks aim to paralyze the charging systems of EVs with malicious traffic, thus rendering the services inaccessible to legitimate users. The disruption of charging services can result in substantial financial losses for electricity providers, inconvenience for users, and potentially environmental damage by disrupting the intended bidirectional flow of energy between EVs and the SG [24].

It is important to note that DoS attacks encompass a variety of techniques, including request flooding, resource exhaustion, and other mechanisms aimed at overloading charging systems, as shown in Table 1. This diversity of attacks underscores the need to develop robust detection and prevention mechanisms against these threats in V2G networks [25].

- Severity and Sophistication of MitM Attacks: MitM attacks represent a major security concern for V2G networks due to their ability to compromise the integrity and confidentiality of data exchanged between Evs and the network. According to a recent study [26], MitM attacks account for over 75% of all data interception attempts in V2G networks. In addition, The MitM attack is ranked among the 8 biggest Cyber threats for 2024 [27]. This attack typically involves an intermediary attacker who intercepts and modifies legitimate communications between the parties involved, often without the sender or recipient being aware of this interception [28].

It is worth noting that MitM attacks encompass a wide range of techniques, including wireless communication interception, identity spoofing, and data falsification as described in Table 2. This diversity of methods highlights the need to implement sophisticated detection mechanisms to identify and mitigate these attacks in V2G networks [20].

In these two attacks, attackers manipulate vehicle authentication data to gain unauthorized access to the V2G network. By falsifying credentials or spoofing vehicle identities, the attackers deceive the network in ordet to accord access to malicious actors. Once inside the network, the attackers can manipulate charging parameters, redirect energy flows, or steal sensitive information such as vehicle registration details, user authentication tokens, and billing information. This scenario prove the importance to find robust mechanisms to prevent unauthorized access and protect the integrity of V2G systems.

With the focus on DoS and MitM attacks, this study comes to improve the security of V2G networks against the most serious and common threats. Indeed, such security breaches can lead to serious consequences, such as significant financial losses, damage to systems or leaks of sensitive data. Therefore, the security of V2G networks is of major importance in the modern era and it is essential to implement effective security measures.

Research teams and developers are constantly working on new solutions to improve the security of V2G networks. Indeed, it is important to continue efforts to address challenges that are also constantly evolving. According to the latest studies [16,20,29-30] modern techniques used to detect anomalies in V2G networks include machine learning, deep learning, and blockchain technology. According to [29,31-32], these techniques have the highest detection rates.

Most IDS proposed for V2G networks are traditional systems that mainly rely on rule-based approaches or generic machine learning models [32-33]. Although these methods are useful, they often fail to adapt to the complex and evolving nature of cyber threats. Indeed, The existing IDS solutions for V2G networks are either too rigid (rule-based) or too resource-demanding (machine learning-based) to effectively handle the dynamic and resource-constrained nature of V2G environments. This creates a pressing need for an IDS that is both adaptive and efficient in real-time threat detection. For example, rule-based IDS, despite their speed, face high false positive rates when confronted with new attack patterns, which is considered a limitation in detecting advanced threats in other network environments. Similarly, while machine learning-based IDS, such as Support Vector Machines (SVM) and Neural Networks (NN), offer improved accuracy, their hardware resource requirements can lead to inefficiencies, particularly in real-time scenarios, as evidenced by the detection delays reported in smart grids.

Our research addresses these gaps by introducing a novel bio-inspired algorithm, the Grouping Cockroach Classifier. The GCC leverages the natural behaviors of cockroaches to distinguish between safe and unsafe shelters (normal and abnormal network activities), providing a robust and adaptive solution. This approach not only improves detection accuracy but also maintains low processing times, making it suitable for real-time V2G applications.

The main objective of this article is to develop an IDS for V2G networks in order to enhance security by identifying and isolating potential threats. This system must be capable of recognizing abnormal and suspicious activities within the network.

The main tool used is the MiniV2G simulator, which accurately emulates the V2G network environment. In addition, MiniEdit serves as a graphical network editor for designing and configuring V2G network topologies, allowing detailed visualization and customization of network scenarios. The Wireshark tool, a network protocol analyzer, is used to capture and inspect network packets in real time, thus facilitating the identification of suspicious activities indicating potential intrusions. Furthermore, CICFlowmeter is used to extract network flow

characteristics, which are essential for detailed traffic analysis as well as the training of datasets and the effective testing of the GCC model.

The implementation of the proposed IDS is primarily carried out in Python, chosen for its flexibility and extensive library support. Key libraries include scikit-learn, used to implement and optimize the GCC model, and networkx, which facilitates the precise modeling of communication structures within V2G networks.

To evaluate the effectiveness of the IDS, various simulation scenarios were tested. The normal operation scenario simulates standard communication and energy exchange between electric vehicles and the grid, without malicious activities, serving as a reference for performance comparison. The attack scenarios include MitM attacks, which involve intercepting and altering communications between vehicles and the grid, and DoS attacks, characterized by overloading network resources with malicious requests to disrupt normal operations. These scenarios are crucial for rigorously testing the IDS's detection and mitigation capabilities.

The system's effectiveness is evaluated based on several key performance measures: detection accuracy (the proportion of correctly identified intrusion attempts), detection time (the average time required to detect an intrusion attempt), and computational cost (the resources required by the IDS during operation, including memory usage and processor load). The results obtained validated the bio-inspired approach of cockroach clustering as a promising binary classification method to improve the security of V2G networks, particularly against DoS and MitM attacks.

2. Related Works

This section presents various approaches proposed in the literature to enhance the security and privacy of V2G networks, evaluating their advantages, limitations, and performance.

Sultana et al. explore IDS based on Software-Defined Networking (SDN) and machine learning approaches [34]. They examine the benefits and limitations of these methods for detecting network attacks. The study emphasizes the importance of feature selection in machine learning to ensure high detection quality. However, limitations of SDN-based IDS and machine learning include challenges in handling large data volumes, selecting optimal parameters for machine learning algorithms, and the need for substantial hardware resources. In summary, while SDN and machine learning can provide powerful intrusion detection tools, it is crucial to consider their limitations and challenges for effective and secure IDS systems.

Roman et al. propose a new solution to address security vulnerabilities in V2G networks by introducing a pairing-based authentication protocol [35]. The protocol aims to resolve issues related to complexity, low security, and resource consumption. Experimental results show advantages in terms of computational and communication costs while ensuring successful authentication. However, challenges remain for practical implementation and addressing security issues in cyber-physical systems. Further exploration of technologies and methods to enhance communication security and protect user identities in EVs is recommended. In summary, this work represents a significant step towards securing V2G networks by proposing a secure authentication protocol with improvements in computational and communication costs. Future efforts should focus on practical protocol implementation and addressing remaining challenges related to cyber-physical system security.

In [36], the authors propose a method to analyze threats associated with the ISO 15118 V2G protocol. This protocol allows electric vehicles to connect to smart grids for energy exchange

and data communication. They evaluate threats at each stage of the ISO 15118 charging negotiation, including the collection and storage of identification data, the exchange of digital certificates, communication of load data, and attacks related to service quality. They suggest security measures such as encryption, digital certificates, digital signatures, firewalls, and access restrictions. This study is important as it provides a detailed analysis of threats related to ISO 15118 protocols, focusing on availability, integrity, authenticity, and confidentiality aspects of communication.

Dudek et al. present a novel communication approach, named "V2G Injector," between EVs and charging stations in V2G networks [37]. This approach transmits data through the power line that supplies EVs and charging stations. The authors describe its operation in detail and evaluate its performance in terms of transmission rate and communication reliability. They demonstrate that V2G Injector establishes reliable communication between EVs and charging stations, providing satisfactory transmission rates. This work contributes to V2G network communication, and its original approach and promising results could inspire further research.

Park et al. demonstrated that a protocol proposed by Shen et al. in 2017 to prevent identity theft, replay attacks, and man-in-the-middle attacks was not effective against various attacks they proposed [38]. However, they developed a key management protocol based on group identities and hash functions to provide robust security and efficient key management in V2G networks. The new protocol offers several advantages, including increased resistance to attacks using dynamic keys and hash algorithms to enhance security. It ensures transmission confidentiality and secure mutual authentication, allowing only authorized users to access information and control vehicles. Despite its advantages, the new protocol also has some limitations, such as the potential need for more hardware resources like bandwidth or computational power to function correctly. Additionally, new attacks could be developed in the future that may compromise the protocol's security.

The authors in [39] conducted an analysis of the features of confidential information in V2G systems to determine their vulnerability to attacks and assess if this information is at risk of disclosure. They used a fuzzy classification technique to develop a fuzzy system. To demonstrate the effectiveness and performance of their fuzzy classification approach, they compared the results with SVM and Naive Bayes) classification techniques. This study presents an innovative methodology for analyzing the security of confidential information in V2G networks using a fuzzy classification approach. However, the study's limitations include testing on a single dataset, which could restrict the generalization of the results.

Su et al. propose an authentication scheme for V2G networks that ensures the confidentiality of sensitive information such as user identities and electric vehicle load data [40]. The proposed authentication scheme uses a combination of encryption and hashing techniques to ensure data confidentiality and authenticity. The study also includes an evaluation of the security of the proposed scheme using formal verification and simulation tools. The advantages of this study include introducing an innovative authentication scheme that ensures the confidentiality of sensitive information and the security of V2G communications. This scheme may help strengthen user trust in V2G networks and encourage the adoption of electric vehicles. However, limitations of this approach may include the complexity of implementing the scheme and the need for a public key infrastructure for key management. Additionally, the article does not provide an analysis of the performance or effectiveness of the proposed scheme compared to other existing approaches.

Basnet et al. proposed an IDS based on deep learning to detect attacks using network traffic data captured at charging stations [31]. The system uses a Convolutional Neural Network (CNN) to extract features from traffic data and a Fully Connected Neural Network (FNN) to classify data into attack or non-attack categories. Experimental results show that the proposed system is effective in detecting attacks and can be used to protect electric vehicle charging stations from cyberattacks. According to the authors, the proposed system can detect intrusions with a precision of 99.9% and a false alarm rate below 0.1%. The average intrusion detection time was approximately 2.2 seconds, which is considered fast. The authors also compared the performance of their IDS with other rule-based intrusion detection and machine learning-based methods, showing that their deep learning system outperformed these other methods in terms of precision and false alarm rates.

The authors in [41] proposed an Adaptive Neuro-Fuzzy Inference System (ANFIS) for assessing the security index in a Vehicular Ad-Hoc Network (VANET). The proposed work is one of the first proposals for attack detection in this type of network. After training the model on data, the proposed system showed good performance in predicting vehicles not under attack and a small error margin in detecting vehicles under attack. However, the authors note that the error margin remains acceptable to ensure the system's effectiveness in predicting attacks using the security index as a protection measure. In conclusion, the authors' proposed model demonstrates that the use of neural networks and fuzzy logic is promising. However, designing an ANFIS model can be complex, requiring a good understanding of fuzzy logic principles and neural networks. Additionally, adjusting model parameters can be challenging to achieve optimal results, potentially requiring longer training times. Despite these challenges, ANFIS remains a powerful tool for predicting security in VANET networks.

The security of the V2G network is a major concern that has led to extensive research and the proposal of several solutions in recent years. The primary threats to the V2G network include issues of confidentiality, authentication, authorization, and billing for electric vehicle charging [32]. Various methodologies, such as machine learning and deep learning algorithms, have been employed to develop intrusion detection systems [6]. Results show that IDS based on these methodologies tend to provide more accurate results than other approaches [16]. However, there are still challenges to overcome to achieve optimal security for the V2G network.

In conclusion, security in V2G networks represents a rapidly evolving field of research. Additional studies are necessary to develop more effective solutions to ensure communication security within these networks, especially considering that attacks are also constantly evolving.

3. IDS

IDS are security tools designed to monitor activities in networks and computer systems to detect abnormal or suspicious behaviors that may indicate an intrusion or attempted attack. These systems can be installed on a computer or network to monitor activities in real-time and send an alert in case of detected anomalies [42].

V2G network is a communication network that allows EVs to connect to the smart electrical grid, providing or receiving electricity while ensuring bidirectional communication with other entities in the network. IDS in V2G networks are designed to monitor activities on this network and detect abnormal or suspicious behaviors. These systems can be installed on electric vehicles and V2G network infrastructures, such as charging stations and network control centers. They monitor real-time activities on the network and can send alerts in case of detected anomalies. These systems are typically used in conjunction with other security measures, such as firewalls

and antivirus software, to protect the V2G network against intrusions and attacks. They play a crucial role in V2G network security, helping to prevent financial losses and avoid damages caused by intrusions and attacks [43].

In this article, we proposed an IDS based on the behavior of cockroaches to classify activities in a V2G network into normal or abnormal activities. We relied on the work presented by Bell et al. in [44-45], in which they presented a biological study on cockroach behavior. The proposed system is based on machine learning to detect and classify abnormal activities such as DoS and MitM attacks in EVCS.

4. Grouping Cockroach Classifier

The classifier utilized in the proposed IDS is inspired by the research conducted by Bell et al. on the social behavior and biological habits of cockroaches [44]. This classifier, known as the Grouping Cockroach Classifier (GCC), is modeled after the natural behavior of cockroaches, particularly their instinct to seek out the most attractive and secure shelter for hiding.

This behavior is thoroughly detailed in an experiment conducted by French biologists as described in [44]. In this experiment, a group of cockroaches was placed in a basin with uniform lighting, and two artificial shelters were created using two red circles, since cockroaches cannot perceive the color red (see Figure 4)

At the beginning of the experiment, the cockroaches moved randomly in all directions, a phase known as the exploration phase. When a cockroach discovered a secure shelter, it would hide there and emit pheromones in the form of odors to signal other cockroaches from the same colony.

By the end of the experiment, it was observed that the cockroaches had a choice between two shelters for hiding (see Figure 5), and they consistently chose the more secure refuge.

4.1. GCC General functioning Process

Figure 6 depicts the overall structure of the GCC, while detailed explanations of each stage follow.

- Darkness of shelters: Cockroaches are naturally drawn to areas of darkness, seeking out most secluded shelters, typically found in corners. The degree of darkness within a shelter is a critical determinant of its perceived safety. Initially, the cockroaches within the training dataset are distributed among their respective shelters, Darkness of shelters is defined in Equation 1.

$$DS(S_i) = \frac{CS_i}{CL} \qquad (1)$$

where :

- $DS(S_i)$: The obscurity rate of the shelter S_i
- CS_i : Number of instances in the shelter S_i
- CL : Total number of instances in all classes.

- Congener attraction: The CA metric, as outlined in Equation 2, is influenced by a predetermined parameter K. When classifying a new instance C_n, K instances (referred to as K congeners for cockroach C_i in shelter S_i) are randomly selected from each class. Then, the total number of instances belonging to this class is divided by the cumulative distance from this instance to its K congeners.

$$CA(C_n, S_i) = \frac{\sum_{1}^{k} dist(C_n, C_k S_i)}{CS_i} \quad (2)$$

where :

- $C_k S_i$: The K^{th} nearest neighbour instance C_n in the class S_i.
- dist(C_n, C_{kS_i}) : Distance between the instances to be classified C_n and its k nearest neighbors in the class S_i.
- k : The number of selected instances.
- CS_i : The total number of instances in the classes S.

- Security quality: The security level, defined in Equation 3, is influenced by the positioning of cockroaches within the shelter; those situated centrally typically experience greater security compared to those located at the shelter's edges. Cockroaches positioned in the middle of the shelter have a higher security rate compared to those positioned at the periphery of the shelter.

$$QS(C_n, S_i) = dist(C_n, BS_i) \quad (3)$$

where :

- BS_i : The centroid of the class S_i.

- Attraction of Shelters: The aggregation operators' outcomes are employed to compute the shelters' attraction for each instance (cockroach) through the following procedure, The formula is presented in Equation 4.

$$SA(C_n, S_i) = \frac{\alpha \times DS(S_i)}{\lambda \times QS(C_n, S_i) + \beta \times CA(C_n, S_i)} \quad (4)$$

where :

- α, β, λ : The adjustment coefficients are used to modify the impact of each operator when calculating the attractiveness of each class.

- Probability of displacement: To determine the probability of displacement, we utilized the naive Bayes algorithm. Bayes' theorem provides a technique to assign a probability to each instance for every potential class. It operates under the assumption that the influence of the value of a predictor X_n on a specific class S_i is unrelated to the values of other predictors. Equation 5 calculates the probability of each instance being classified into class S_i:

$$P(C_n, S_i) = P(X_i, S_i) \times P(X_2, S_i) \times \ldots P(S_i) \quad (5)$$

where :

- $P(C_n, S_i)$: The probability that the instance C_n is classified in the class S_i.
- $P(Si)$: Is the prior probability of the class S_i.
- $P(x \mid Si)$: Is the probability that component X generates the class S_i.

- Classification: Each incoming instance (cockroach) is assigned to the class (shelter) with the greatest attraction, indicating the highest likelihood of membership. The security function $f(C_i, S_i)$, detailed in Equation 6, assists in identifying the optimal class for each instance (the most secure shelter S_i for each cockroach C_n). The final determination of each instance's class is based on the evaluation of the security function.

$$f(C_n, S_i) = P(C_n, S_i) + SA(C_n, S_i) \quad (6)$$

where :

- $SA(C_i, S_i)$: The attraction of the class S_i for the instance C_n.
- $P(C_i, S_i)$: The probability of the cockroach C_i to be classified in the class S_i.

Each instance is assigned to the shelter with the highest value of the safety function.

- Iterative Calculation: Following each iteration's conclusion, the aggregation rule values and the likelihood of movement for each instance undergo updates. In cases of misclassification, efforts are made to relocate the instance to a safer shelter. This iterative process continues until the stopping criterion is met.
- Stopping Criterion: If the predetermined number of iterations is reached, or if the number of instances in each class remains unchanged between iterations i and $i+1$.

In this classification scenario, the dataset is partitioned into two segments: the training set and the test set. Each new instance (cockroach) is then classified within a class (shelter) utilizing a security function reliant on the attractiveness of each class. This attractiveness is determined by considering factors such as the darkness level of the shelter, congener attraction, and security quality. The likelihood of movement is computed using the Naive Bayes algorithm.

5. Methodology

We used the MiniV2G emulator to simulate various V2G networks, both with and without attacks, for the construction of our dataset. MiniV2G was developed by Luca Attanasio et al. [46]. It is a derivative of Mininet-WiFi, which itself is based on Mininet, specially designed for simulating V2G environments by integrating with RiseV2G. MiniV2G acts as a platform for emulating V2G power networks using Mininet, thus creating a electric vehicle network.

MiniEdit, an adjunct tool for Mininet, facilitates the design, configuration, and testing of topologies via an intuitive drag-and-drop graphical interface. Through the combined use of MiniV2G and MiniEdit, users can design network topologies that incorporate electric vehicles and charging stations, leveraging the enhanced user interface provided by MiniV2G. MiniEdit, an adjunct tool for Mininet, facilitates the design, configuration, and testing of topologies via

an intuitive drag-and-drop graphical interface. Through the combined use of MiniV2G and MiniEdit, users can design network topologies that incorporate electric vehicles and charging stations, leveraging the enhanced user interface provided by MiniV2G.

5.1. Generation of Dataset

In this section, we delineate the methodology employed to procure the attack database and outline the procedure for selecting significant variables. We utilized the MiniV2G simulator, Wireshark, and CICFlowMeter software to generate the attack database. Subsequently, Principal Component Analysis (PCA) was employed to cleanse this database, and the most pertinent variables were identified using the Weka tool (Weka stands for Waikato Environment for Knowledge Analysis).

Detecting attacks in networks, particularly in V2G networks, necessitates an attack database derived from the exchange of information among network entities. This database must be generated through multiple simulations. The MiniV2G tool, an open-source solution proposed by Luca Attanasio et al. [46], facilitated the simulation of a V2G environment while adhering to ISO 15118 standard specifications. Simulations were conducted based on three distinct scenarios:

- **First Scenario** : In this attack-free scenario, depicted in Figure 7, the V2G network includes two electric vehicles (ev1 and ev2), one charging station (se1), a switch (s1), and a controller (c0).

- **Second Scenario** : In this scenario, an attacker intercepts communications between electric vehicles and the V2G network, exploiting vulnerabilities in data transmission protocols. The attacker manipulates the data packets exchanged between the vehicles and the network, potentially altering critical information such as charging schedules, energy pricing data, vehicle authentication tokens, and vehicle identification numbers (VINs). By tampering with this data, the attacker can disrupt the normal operation of the V2G system, leading to financial losses for energy providers and inconvenience for users .This scenario, featuring a MitM attack, is depicted in Figure 8. The goal of the MitM attacker is to intercept outgoing traffic from the Electric Vehicle (EV) with the possibility to perform any necessary manipulations before forwarding the flow to the charging station (SE). The V2G network in this scenario is composed of an electric vehicle (ev1), a switch (s1), a charging station (se1), and a MitM attacker (mitm).

- **Third Scenario** : In this scenario, attackers launch a coordinated DoS attack against the charging infrastructure of V2G networks. By flooding the charging stations with a high volume of malicious requests, the attackers paralyze the system's resources, rendering it unavailable for legitimate users. The DoS attack may target critical components of the charging infrastructure, such as billing systems, authentication servers, and communication interfaces. By disrupting the availability of these systems, the attackers disrupt the charging process and cause financial losses for energy providers .For the DOS-attack scenario depicted in Figure 9, the hacker sends multiple requests continuously to the controller and the charge station until the targeted network service is disrupted. In this case, the V2G network is composed of an electric vehicle (ev1), a charge station (se1), a switch (s1), and a Dos attacker.

In these scenarios described, Wireshark was employed to capture network flows and monitor the interfaces of each communication point during the electric vehicle charging process. For

each scenario, the charging process was simulated multiple times to collect a sufficient number of packets. After organizing the interfaces, the data was saved in packet capture (PCAP) format. At the end, three PCAP files were generated following the simulations of these three scenarios. To convert the collected data into CSV format, the CICFlowMeter tool was used.

CICFlowMeter is well-known for its ability to generate datasets related to attacks [6,47]. We used CICFlowMeter to create three partial databases. Each partial database for each scenario is saved in CSV format with 84 labeled columns for each flow, such as: FlowID, SourceIP, DestinationIP, SourcePort, DestinationPort, Protocol, etc.

After obtaining three partial databases corresponding to the three simulated scenarios, we added a new column, ATT (for ATTack), to distinguish the data captured in the scenario without an attack from that captured in the scenario with an attack. In the database file for the scenario without an attack, the variable ATT is set to 0. Conversely, in the files representing the databases for scenarios involving a MitM attack and a DoS attack, the variable ATT is set to 1.

Finally, after incorporating the ATT attribute, the three partial databases were combined into a single comprehensive database containing 85 labeled columns (84 columns generated by CICFlowMeter plus the ATT column).

5.2. Selection of Significant Variables

The degree to which different variables in the database contribute to predicting the binary ATT variable varies significantly. Some variables are more influential than others in this prediction. To avoid dealing with all the variables obtained, we identified the most significant ones. This step helped us to minimize data redundancy and reduce the time required for classification processes.

We utilized Principal Component Analysis (PCA) using Weka 8.3.4 software to identify the most significant variables. According to the Weka tool, the significant variables include Tot Fwd Pkts, Flow Pkts, Fwd IAT std, Fwd Pkts/s, Bwd Pkts/s, and Idle Min. These variables are detailed in Table 3.

6. Results and discussion

6.1. Performance Measurement Criteria

The confusion matrix is a metric widely used in the validation of intrusion detection systems. It is commonly used to evaluate the classification performance of activities in a network. The principle of the confusion matrix is based on four key elements described below. The confusion matrix model is presented in Table 4:

- True Positive (TP): Normal samples correctly classified as normal traffic.
- False Negative (FN): Normal samples incorrectly classified as abnormal traffic.
- False Positive (FP): Number of abnormal samples incorrectly classified as normal traffic.
- True Negative (TN): Number of abnormal samples correctly classified as abnormal traffic.

It should be noted that there are several metrics used to evaluate an intrusion detection model. In this study, we selected the most representative metrics to evaluate the performance of the proposed IDS, these metrics are: ACC, PR, F-value, DR and FPR, defined below.

- **Accuracy (ACC)**: The ratio of correctly classified samples to the total number of samples. The formula for ACC is presented in Equation 7.

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \quad (7)$$

- **Precision (PR)**: The percentage of normal traffic correctly classified among normal traffic samples. Its formula is presented in Equation 8.

$$PR = \frac{TP}{TP + FP} \quad (8)$$

- **Detection Rate (DR):** Defines the quotient between the number of correctly identified abnormal activities and total number of abnormal activities. The detection rate reflects the ability of the proposed IDS to correctly identify attacks. The formula is presented in Equation 9.

$$DR = \frac{TP}{TP + FN} \quad (9)$$

- **F-Value**: Represents the harmonic mean of Precision and Detection Rate. Its formula is presented in Equation 10.

$$F\text{-}Value = 2 \times \frac{PR \times DR}{PR + DR} \quad (10)$$

- **False Positive Rate (FPR)**: The ratio of incorrectly identified abnormal samples to the predicted number of normal samples. Its formula is presented in Equation 11.

$$FPR = \frac{FP}{FP + TP} \quad (11)$$

6.2. Results Analysis

To evaluate the performance of the GCC classifier, experiments were carried out in binary classification scenarios to predict the binary variable Att. The classifier was trained on the training sets from the generated dataset, which comprised 70% of the inputs (refer to Section 5.1). The validation set (10%) was used for optimization and parameter tuning, while the test set, consisting of 20% of the inputs, was used to determine the error rate of the optimized classifier, thus evaluating its performance. The results obtained after 50 iterations are presented in Table 5.

- $ACC = \frac{7707 + 6702}{7707 + 6702 + 59 + 96} = 0.9893 = 98.93\%.$
  A prediction rate of 98.93%, corresponding to an error rate of 0.0107%

- $DR = \frac{7707}{7707 + 96} = 0.9876 = 98.76\%.$
  The result of the ACC obtained translates into the capacity of the proposed model to predict all the data related to attacks.

- $PR = \frac{7707}{7707+59} = 0.9924 = 99.24\%$.
  This result indicates that 99.24% of the entries detected as attacks are indeed attacks.

- $F-Value = 2 \times \frac{0.9924 \times 0.9876}{0.9924+0.9876} = 0.9899 = 98.99\%$
- $FPR = \frac{FP}{FP+TP} = \frac{59}{59+7707} = 0.0075 = 0.75\%$
  This represents the proportion of abnormal activities that were incorrectly identified as normal among all the activities predicted to be normal in the network.

Among the diverse results obtained, the intrusion detection model utilizing the GCC classifier provides a highly satisfactory results.

6.3. Evaluation of the proposed IDS with other Datasets

In this section, the performance and precision of the proposed model are evaluated using additional datasets commonly employed for evaluating intrusion detection performance. The following datasets are presented:

- KDD CUP99 : Since 1999, KDD Cup 99 has been used as a benchmark dataset in behavioral intrusion detection systems. Each packet in the KDD Cup 99 dataset consists of 41 fields and is labeled as either a normal packet or an abnormal packet with specific attack types [48].
- NSL_KDD : is a new dataset, representing a continuation of the KDD'99 dataset version. It is designed as an effective benchmark dataset to assist researchers in comparing various intrusion detection methods [49].
- UNSW_NB15 : is a widely utilized dataset in the field of network intrusion detection. This database incorporates various attacks, including DoS, worms, backdoors, and fuzzers. The dataset comprises 175,341 records in the training set and 82,332 records in the testing set, encompassing a range of scenario types [50].
-

To perform binary classification (normal and abnormal network activities), we introduced the Att attribute (Att for Attack) to each datasets. The Att attribute takes the following values:

- Att = 0: Normal network flow
- Att = 1: Abnormal network flow

In order to verify the performance of GCC classifier used in the proposed model, we conducted experiments with binary classification scenarios, using the training sets in KDD CUP99, NSL_KDD, and UNSW_NB15 datasets to train the classifier, then we used the test sets to calculate the accuracy of the classifier and evaluating its performances.

From Figure 10, we can comclude that the proposed IDS using the GCC classifier maintains its effectiveness when applied to different Datasets. Specifically, for the KDD CUP99 dataset, the IDS achieves 98% accuracy in detecting normal traffic and 97.8% accuracy in identifying attacks. With the NSL_KDD dataset, the accuracy rate for both normal traffic and attack detection is 99%. For the UNSW_NB15 database, the IDS attains 95.8% accuracy in detecting attacks and 93.5% accuracy for normal traffic. These results confirm that the proposed model assure high performance and precision.

6.4. Comparative experiments

In this section, we present a comparative study between the proposed model and other models from previous research. Using Weka software, which includes a variety of classifiers, we selected the following classifiers to compare against our proposed GCC-based model:

- Long-Short Term Memory (LSTM)
- Support vector machines (SVMs)
- Deep Belief Network (DBN)
- Convolutional Neural Network (CNN)
- CNN based Auto Encoder (CNN-AE)

To further evaluate the proposed IDS based on the GCC classifier, we conducted experiments to compare our method with other approaches previously discussed in the literature. These experiments were performed on the same Dataset. We individually examined the ACC, DR, and FPR measurements, and the results of this comparative analysis are detailed in Figure 11.

The comparison results, shown in Figure 11, demonstrate that the proposed model has indeed improved its performance in terms of ACC, DR and FPR compared to other models in previous studies. The used model achieved an ACC value of 98.93%, significantly exceeding the ACC values of other approaches. The DR value reached 98.76%, the highest among all evaluated methods. While the FPR of our model is 0.75%, which is much higher than the FPR provided by the LSTM classifier. Overall, the model proposed in this paper significantly improves the detection rate and accuracy of the intrusion detection system while significantly reducing the false positive rate. These results confirm the superiority of the proposed model compared to other models described in previous studies. Additionally, it demonstrates improved adaptability to various network attack scenarios. In the field of intrusion detection, the proposed model optimizes efficiency without altering precision.

6.5. Comparative Analysis

To further evaluate the effectiveness of the GCC Classifier against existing techniques, we conducted a series of experiments comparing its performances with rule-based IDS and machine learning-based IDS, specifically Support Vector Machines (SVM) and Neural Networks (NN). Each model was implemented and tested using the same Dataset, which included both legitimate and malicious traffic instances generated from simulated V2G environments. Key performance metrics evaluated include detection accuracy, false positive rate, resource utilization, and processing time.

The experiments were conducted on a machine with the specifications presented in Table 6.

From Figure 12, we can conclude that machine learning approaches like SVM and NN offer better accuracy than rule-based IDS but at the cost of higher processing times and resource utilization. The GCC keeps a balance by providing high ACC and low FPR with moderate resource usage and efficient processing times (see Section 6.6), making it particularly suitable for real-time V2G applications.

6.6. Comparative Study of Processing Time

The processing time for each model was measured as the average time required to process a single instance of network traffic data. The processing times for the GCC and the other IDS models are summarized in Table 7 and depicted in Figure 13:

Based on the results presented in Table 7, the GCC classifier showed an average processing time of 0.05 seconds per instance. This balance between efficiency and effectiveness is achieved by the bio-inspired nature of the algorithm, which uses the behavioural heuristics of cockroaches to rapidly classify network activities as either normal or abnormal. In contrast, the rule-based IDS is the fastest in terms of processing time at 0.02 seconds per instance. However, it is important to note that while this model is efficient in terms of computational complexity, it often lacks the precision, the robustness and the adaptability necessary to accurately detect sophisticated and evolving cyber threats. The SVM-based IDS showed an average processing time of 0.10 seconds per instance. Although SVMs are powerful for classification tasks, their computational complexity can lead to longer processing times, especially with large and complex Datasets. Finally, the neural network-based IDS had an average processing time of 0.08 seconds per instance. While neural networks are effective in learning complex patterns, they require significant computational resources, which can result in longer processing times compared to simpler models like the rule-based IDS.

The graph in Figure 14 illustrates the processing times for different IDS models over 100 instances. The GGC Classifier maintains a relatively stable processing time around 0.05 seconds per instance with a high ACC, demonstrating its consistency and efficiency. The Rule-Based IDS shows the fastest processing times, averaging around 0.02 seconds per instance but with with lack of precision. The SVM-Based IDS and NN-Based IDS need higher processing times, averaging around 0.10 and 0.08 seconds per instance, respectively, reflecting their greater computational demands.

7. Conclusion

The integration of electric vehicles into smart grids, known as Vehicle-to-Grid (V2G), requires the implementation of robust security measures to protect the network against serious threats such as MitM and DoS attacks. These attack types pose significant risks to the V2G process, potentially affecting the stability, security, and reliability of the grid and the connected vehicles. Thus, effective intrusion detection and mitigation strategies are essential to protect the network against these threats.

Most IDS proposed for V2G networks are traditional systems that primarily rely on rule-based approaches or generic machine learning models. Although these methods are useful, they often fail to adapt to the complex and evolving nature of cyber threats. Therefore, there is a need to find more effective solutions to protect the network.

This article proposes an intrusion detection system inspired by the biological behavior of cockroaches in their search for safe shelters. It begins with the generation of a dataset representing both normal and abnormal traffic, allowing for precise experiments and evaluations of the proposed model. The model achieves an accuracy rate of approximately 98.93%, demonstrating its effectiveness in identifying potential intrusions.

For further validation, we tested the GCC classifier on other datasets widely used in IDS evaluation, including KDD CUP99, NSL_KDD, and UNSW_NB15. The results demonstrated the model's effectiveness and high accuracy in detecting abnormal activities within networks. Additionally, we compared our intrusion detection system with other approaches in the literature in terms of performance metrics such as detection accuracy, false positive rate, resource utilization, and processing time. The comparison results show that our model strikes a

balance by providing high accuracy and low false positive rates with moderate resource usage and efficient processing times, making it particularly suitable for real-time V2G applications.

The high accuracy and efficiency demonstrated by the proposed model highlight its importance in improving the security of V2G networks, playing a crucial role in the sustainable development and security of modern electric transportation systems.

References

1. Yuan, J. Lu, Y. Wang, C. et al. "Ecology of industrial pollution in China". *Ecosystem Health and Sustainability*, 6(1), 1779010 (2020). DOI:10.1080/20964129.2020.1779010
2. Demiral, M. Haykir, O. and Aktekin-Gok, E. D. "Environmental pollution effects of economic, financial, and industrial development in OPEC: Comparative evidence from the environmental Kuznets curve perspective". *Environment, Development and Sustainability*, pp. 1-32 (2023). DOI:10.1007/s10668-023-03663-6
3. Wu, T. Cui, Y. Lian, A. et al. "Vehicle emissions of primary air pollutants from 2009 to 2019 and projection for the 14th five-year plan period in Beijing, China". *Journal of Environmental Sciences*, 124, pp. 513-521 (2023). DOI:10.1016/j.jes.2021.11.038
4. Vadi, S. Bayindir, R. Colak, A. M. et al. "A review on communication standards and charging topologies of V2G and V2H operation strategies". *Energies*, 12(19), 3748 (2019). DOI:10.3390/en12193748
5. Johnny, X. Chris, J. and Marcy, R. "Global electric vehicle market 2020 and forecasts". *Canalys Newsroom* (2021).
6. Nonvignon, T. Z. Boucif, A. B. and Mhamed, M. "A copula-based attack prediction model for vehicle-to-grid networks". *Applied Sciences*, 12(8), 3830 (2022). DOI:10.3390/app12083830
7. Iqbal, S. Habib, S. Ali, M. et al. "The impact of V2G charging/discharging strategy on the microgrid environment considering stochastic methods". *Sustainability*, 14(20), 13211 (2022). DOI:10.3390/su142013211
8. Pal, A. Bhattacharya, A. and Chakraborty, A. K. "Placement of electric vehicle charging station and solar distributed generation in distribution system considering uncertainties". *Scientia Iranica*, 30(1), 183-206 (2023). DOI:10.24200/sci.2021.56782.4908
9. Observations, A. L. and Des, L. A. N. "Road vehicles-to-grid communication interface-part 2: network and application protocol requirements" (2014). DOI:15118-2:2014
10. Hecht, C. Figgener, J. and Sauer, D. U. "Protocols and interfaces for EV charging". *In Next Generation Electrified Vehicles Optimised for the Infrastructure*, pp. 77-89. Cham: Springer Nature Switzerland (2024). DOI:10.1007/978-3-031-47683-9_7
11. Bilal, M. and Rizwan, M. "Intelligent algorithm-based efficient planning of electric vehicle charging station: A case study of metropolitan city of India". *Scientia Iranica*, 30(2), 559-576 (2023). DOI:20.1001.1.10263098.2023.30.2.15.4
12. Owens, J. Miller, I. and Gencer, E. "Can vehicle-to-grid facilitate the transition to low carbon energy systems?". *Energy Advances*, 1(12), pp. 984-998 (2022).DOI:10.1039/D2YA00204C
13. Conti, M. Donadel, D. Poovendran, R. et al. "Evexchange: A relay attack on electric vehicle charging system". *In European Symposium on Research in Computer Security*. pp. 488-508. Cham: Springer International Publishing (2022, September). DOI:10.1007/978-3-031-17140-6_24
14. Kumar, G. and Mikkili, S. "Critical review of vehicle-to-everything (V2X) topologies: Communication, power flow characteristics, challenges, and opportunities". *CPSS Transactions on Power Electronics and Applications* (2023). DOI: 10.24295/CPSSTPEA.2023.00042
15. Brighente, A. Conti, M. Donadel, D. et al. "Electric vehicles security and privacy: challenges, solutions, and future needs". *arXiv preprint arXiv*:2301.04587 (2023). DOI:10.48550/arXiv.2301.04587
16. Du, J. Yang, K. Hu, Y. et al. "Nids-cnnlstm: Network intrusion detection classification model based on deep learning". *IEEE Access*, 11, pp. 24808-24821 (2023). DOI:10.1109/ACCESS.2023.3254915

17. Heidari, A. and Jabraeil, Jamali, M. A. "Internet of things intrusion detection systems: A comprehensive review and future directions". *Cluster Computing*, pp. 1-28 (2022). DOI:10.1109/ACCESS.2023.3254915
18. Aslan, O. Aktug, S. S. Ozkan-Okay, M. et al. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions". *Electronics*, 12(6), 1333 (2023). DOI:10.3390/electronics12061333
19. Pali, I. Amin, R. and Abdussami, M. "Autonomous vehicle security: Current survey and future research challenges". *Security and Privacy*, 7(3), e367 (2024). doi.org/10.1002/spy2.367
20. Niroumand, F. J. Bonab, P. A. and Sargolzaei, A. "Security of connected and autonomous vehicles: A review of attacks and mitigation strategies". *SoutheastCon*, 1197-1204 (2024). DOI:10.1016/j.cose.2020.102150
21. Kaiser, F. Shulman, H. and Waidner, M. "Poster: longitudinal analysis of DoS attacks". *In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. pp. 3573-3575 (2023). doi.org/10.1145/3576915.3624382
22. Saba, I. Bukhari, M. Ullah, M. et al. "Threats, vulnerabilities, and mitigation in V2G networks". *In Planning and Operation of Electric Vehicles in Smart Grids*. pp. 1-30. Cham: Springer Nature Switzerland (2023). DOI:10.1007/978-3-031-35911-8_1
23. Hamdare, S. Kaiwartya, O. Aljaidi, M. et al. "Cybersecurity risk analysis of electric vehicles charging stations". *Sensors*, 23(15), 6716 (2023). DOI:10.3390/s23156716
24. Rajasekaran, A. S. Azees, M. and Al-Turjman, F. A "Comprehensive survey on security issues in vehicle-to-grid networks". *Journal of Control and Decision*, 10(2), 150-159 (2023). DOI:10.1080/23307706.2021.2021113
25. Priyanka, S. and Vijay Bhanu, S. "A survey on variants of DoS attacks: Issues and defense mechanisms". *Journal of applied research and technology*, 21(1), 12-16 (2023). doi.org/10.22201/icat.24486736e.2023.21.1.2166
26. Riggs, H. Tufail, S. Parvez, I. et al. "Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure". *Sensors*, 23(8), 4060 (2023). DOI:10.3390/s23084060
27. Leconte, Y. "Rapport sur les menaces DDoS au quatrième trimestre 2024". https://blog.cloudflare.com/ddos-threat-report-2023-q4-fr-fr . published avril 30, 2024. Accessed: May 20, 2024.
28. Taslimasa, H. Dadkhah, S. Neto, E. C. P. et al. "Security issues in internet of vehicles (IoV): A comprehensive survey". *Internet of Things*, 100809 (2023). DOI:10.1016/j.iot.2023.100809
29. Abdullahi, M. Baashar, Y. Alhussian, H. et al. "Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review". *Electronics*, 11(2), 198 (2022). DOI:10.3390/electronics11020198
30. Fellah, A. Mekkaoui, K. Zehaf, A. et al. "Investigating the effectiveness of Word2Vec for spam detection using lazy predict library", *Int J Intell Syst Appl Eng*, vol. 12, no. 3, pp. 2968–2977 (2024). https://ijisae.org/index.php/IJISAE/article/view/5887
31. Basnet, M. and Ali, M. H. "Deep learning-based intrusion detection system for electric vehicle charging station". *In 2020 2nd International Conference on Smart Power and Internet Energy Systems (SPIES)*, pp. 408-413. IEEE (2020). DOI:10.1109/SPIES48661.2020.9243152
32. Javed, M. Arslan, A. M. Noor, M. A. et al. "On the security of a novel privacy-preserving authentication scheme for V2G networks". *Security and Privacy*, *7*(2), e357 (2024). doi.org/10.1002/spy2.357
33. Warraich, Z. S. and Morsi, W. G. "Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids". *Sustainable Energy, Grids and Networks*, 34, 101027 (2023). DOI:10.1016/j.segan.2023.101027
34. Sultana, N. Chilamkurti, N. Peng, W. et al. "Survey on SDN based network intrusion detection system using machine learning approaches". *Peer-to-Peer Networking and Applications*, 12(2), 493-501 (2019). DOI:10.1007/s12083-017-0630-0
35. Roman, L. F. Gondim, P. R. and Loret, J. "Pairing-based authentication protocol for V2G networks in smart grid". *Ad Hoc Networks*, 90, 101745 (2019). DOI:10.1016/j.adhoc.2018.08.015
36. Bao, K. Valev, H. Wagner, M. et al. "A threat analysis of the vehicle-to-grid charging protocol ISO 15118". *Computer Science-Research and Development*, 33(1-2), pp. 3-12 (2018). DOI:10.1007/s00450-017-0342-y

37. Dudek, S. Delaunay, J. C. and Fargues, V. "V2G injector: whispering to cars and charging units through the power-line". *In Proceedings of the SSTIC (Symposium sur la securite des technologies de l'information et des communications)*, Rennes, France, pp. 5-7 (2019).
38. Park, K. Park, Y. Das, A. K. et al. "A dynamic privacy-preserving key management protocol for V2G in social internet of things". *IEEE Access*, 7, pp. 76812-76832 (2019). DOI:10.1109/ACCESS.2019.2921399
39. Kaya, G. A. and Badwan, A. "Fuzzy rule based classification system from vehicle-to-grid data". *In 2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-7. IEEE (2021). DOI: 10.1109/ISDFS52919.2021.9486370
40. Su, Y. Shen, G. and Zhang, M. "A novel privacy-preserving authentication scheme for V2G networks". *IEEE Systems Journal*, 14(2), pp. 1963-1971 (2019). DOI: 10.1109/JSYST.2019.2932127
41. Bensaber, B. A. Diaz, C. G. P. and Lahrouni, Y. "Design and modeling an adaptive neuro-fuzzy inference system for the prediction of a security index in VANET". *Journal of Computational Science*, 47, 101234 (2020). DOI:10.1016/j.jocs.2020.101234
42. Mekkaoui, K. and Meddah, I. "Performances evaluation of threshold-based IDS and trust based IDS under smart black hole attacks". *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 14(1), pp. 154-166 (2023). DOI:10.61841/turcomat.v14i1.13388
43. Rajasekaran, A. S. Azees, M. and Al-Turjman, F. "A comprehensive survey on security issues in vehicle-to-grid networks". *Journal of Control and Decision*, 10(2), pp. 150-159 (2023). DOI:10.1080/23307706.2021.2021113
44. Bell, W. J. Roth, L. M. and Nalep, C. A. "Cockroaches: ecology, behavior, and natural history". *JHU Press* (2007). DOI:10.1353/book.3295
45. Boukhalfa, S. Amine, A. and Hamou, R. M. "Border security and surveillance system using IoT". *International Journal of Information Retrieval Research (IJIRR)* 12(1), pp. 1-21 (2022). DOI:10.4018/IJIRR.289953
46. Attanasio, L. Conti, M. Donadel, D. et al. "MiniV2G: An electric vehicle charging emulator". *In Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*, pp. 65-73 (2021). DOI:10.1145/3457339.3457980
47. Ali, B. H. Sulaiman, N. Al-Haddad, S. A. R. et al. "DDoS detection using active and idle features of revised CICFlowMeter and statistical approaches". *In 2022 4th International Conference on Advanced Science and Engineering (ICOASE)*, pp. 148-153. IEEE (2022). DOI:10.1109/ICOASE56293.2022.10075591
48. Kumar, S. Gupta, S. and Arora, S. "A comparative simulation of normalization methods for machine learning-based intrusion detection systems using KDD Cup'99 dataset". *Journal of Intelligent and Fuzzy Systems*, 42(3), pp. 1749-1766 (2022). DOI:10.3233/JIFS-211191
49. Solekha, N. A. "Analysis of NSL-KDD dataset for classification of attacks based on intrusion detection system using binary logistics and multinomial logistics". *In Seminar Nasional Official Statistics*, Vol. 2022, No. 1, pp. 507-520 (2022). DOI:10.34123/semnasoffstat.v2022i1.1138
50. Sallam, Y. F. Abd El-Nabi, S. El-Shafai, W. et al. "Efficient implementation of image representation, visual geometry group with 19 layers and residual network with 152 layers for intrusion detection from UNSW-NB15 dataset". *Security and Privacy*, 6(5), e300 (2023). DOI:10.1002/spy2.300

Figure and Table captions

Figures	Tables
Figure 1. Estimated electric vehicle sales by 2030.	Table 1. Type of DoS attacks
Figure 2. V2G communication Actors	Table 2. Type of MitM attacks
Figure 3. DoS attack statistics.	Table 3. Significant variables
Figure 4. Description of the cockroach grouping experiment	Table 4. Confusion Matrix
Figure 5. The grouping of cockroaches under the same place	Table 5. Confusion Matrix of the proposed IDS
Figure 6. GCC general functioning process	Table 6. Machine Performances
Figure 7. Scenario without attack	Table 7. Average Processing Time
Figure 8. Scenario with MitM attack	
Figure 9. Scenario with Dos attack	
Figure 10. Classification Accuracy (ACC)	
Figure 11. Performance comparison	
Figure 12. Comparative Analysis	
Figure 13. Average Processing Time.	
Figure 14. Processing Times for Different IDS Models Over Time.	

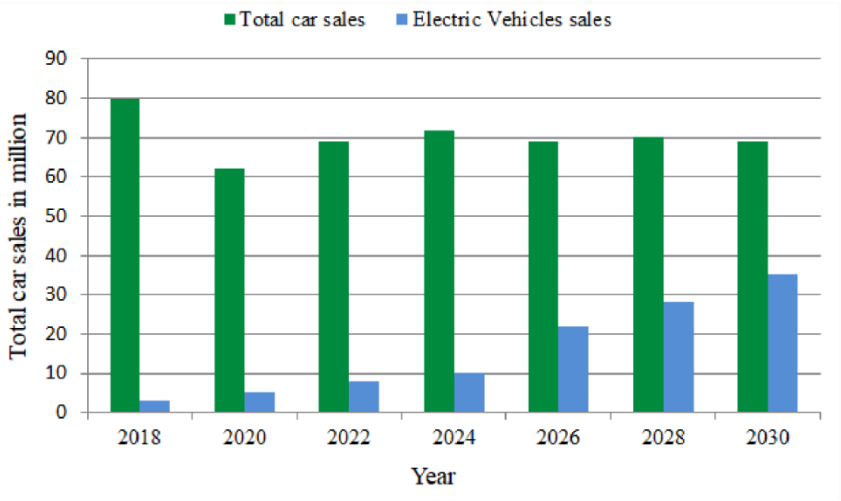


Figure 1. Estimated electric vehicle sales by 2030.

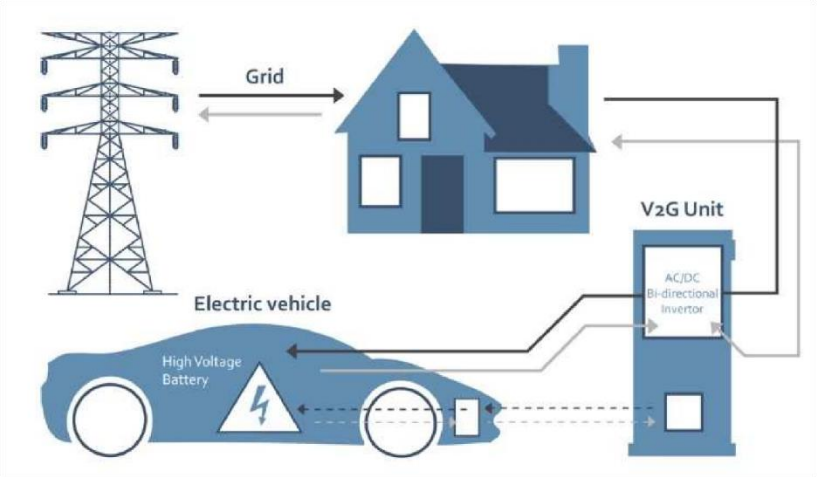


Figure 2. V2G communication Actors

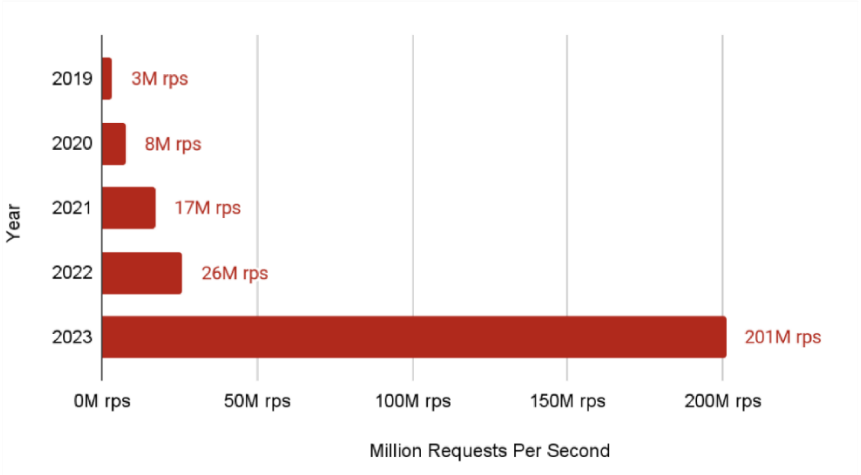


Figure 3. DoS attack statistics

Attack	Description
Request Flooding	Inundating V2G servers with a large number of requests in order to paralyze resources and rende the service unavailable.
Resource Exhaustion	Intentionally consume the system resources of V2G servers, causing slowdowns or complete system shutdowns.
Amplification Attacks	Exploiting misconfigured protocols to generate excessive traffic towards the target.
Fragmentation Attacks	Fragmenting network packets to exhaust the resources of the target system
Congestion Attacks	Manipulating network traffic to create artificial congestions, disrupting the normal flow of data.

Table 1. Type of DoS attacks

Attack	Description
Wireless Interception	Intercepting wireless communications between electric vehicles and the V2G network in order to disclose the confidentiality of data.
ARP Spoofing	Falsifying ARP protocol addresses to intercept and modify network traffic.
DNS Spoofing	Falsifying DNS server responses, redirecting queries to malicious destinations.
Relay Attacks	Relaying communications between legitimate parties to intercept or modify exchanged data.
Identity Spoofing	Impersonating a legitimate V2G network node, allowing unauthorized access to the system.
Redirection Attacks	Redirecting legitimate network traffic to unauthorized destinations, disrupting normal communications.

Table 2. Type of MitM attacks

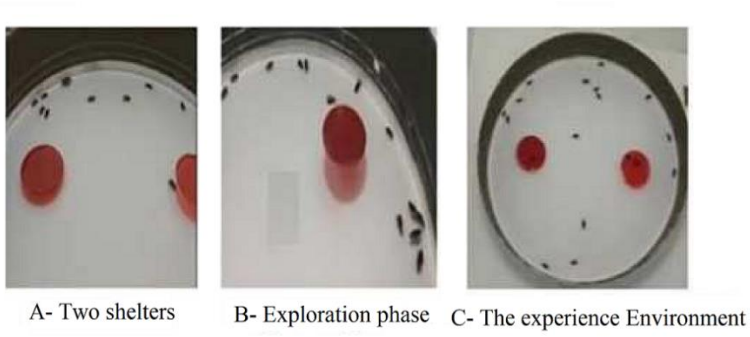


Figure 4. Description of the cockroach grouping experiment

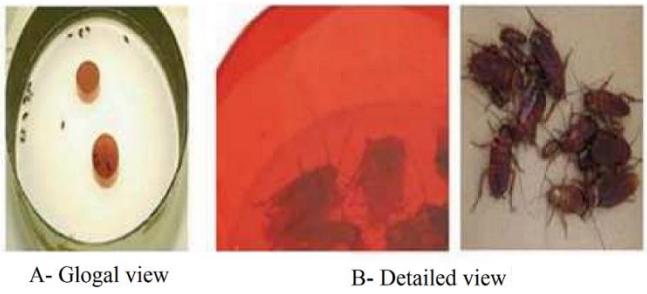


Figure 5. The grouping of cockroaches under the same place

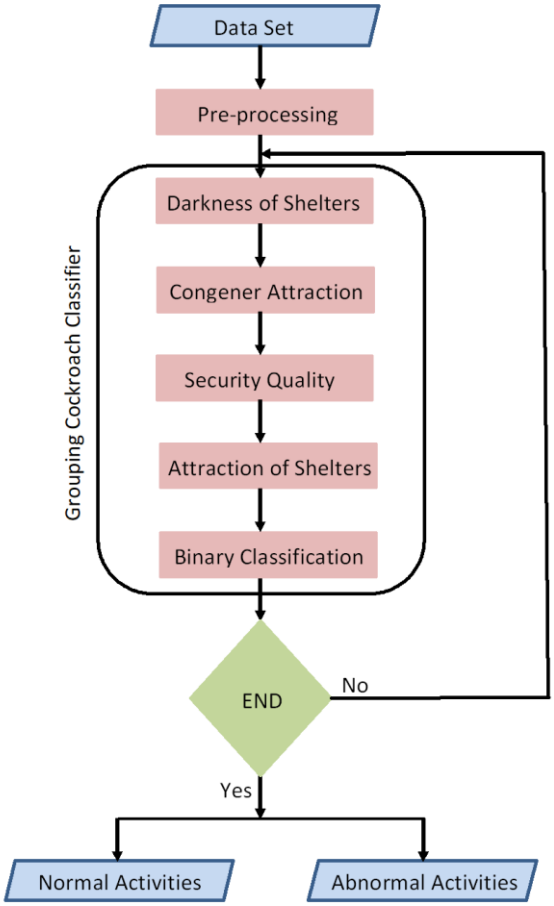


Figure 6. GCC general functioning process

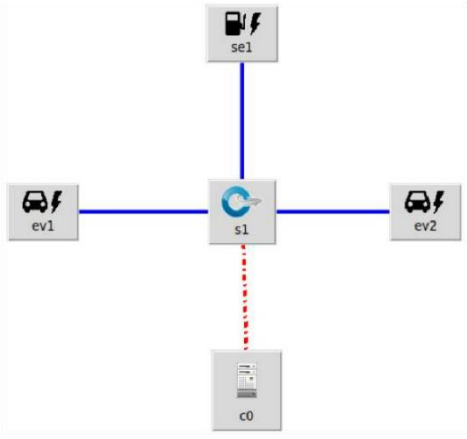


Figure 7. Scenario without attack

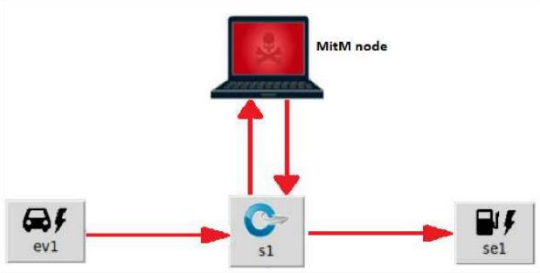


Figure 8. Scenario with MitM attack

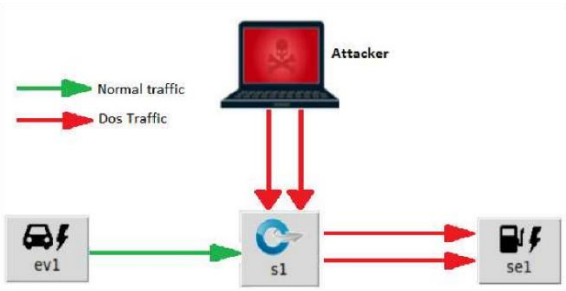


Figure 9. Scenario with Dos attack

Variables	Description
Tot Fwd Pkts	Total packets in the forward direction
Flow Pkts	packet rate which is the number of packets transferred per second
Fwd IAT std	time difference between two flows
Fwd Pkts/s	standard deviation size of the packet in the forward direction
Bwd Pkts/s	standard deviation size of the packet in the indirect direction
Idle Min	minimum time a flow was inactive before becoming active

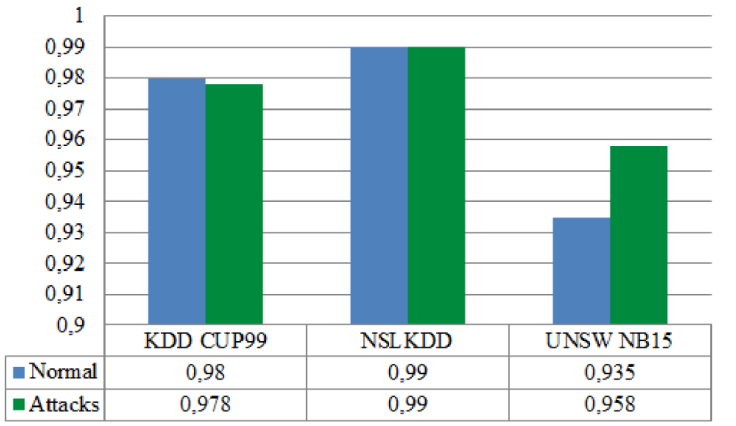
Table 3. Significant variables

		Prediction category	
		Positive	**Negative**
Real category	**Positive**	TP	FN
	Negative	FP	TN

Table 4. Confusion Matrix

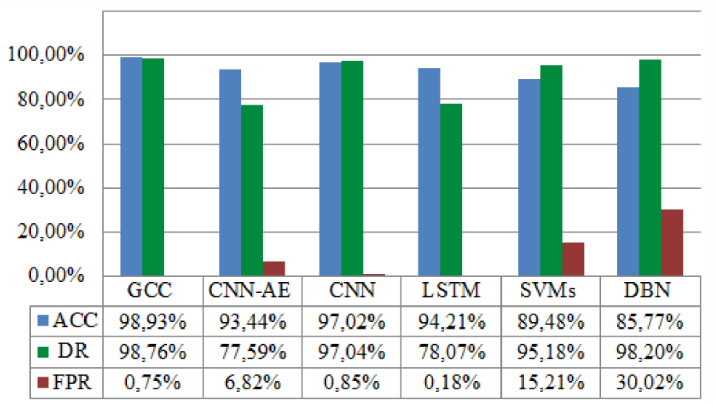
		Prediction category	
		1	**0**
Real category	**1**	7707	96
	0	59	6702

Table 5. Confusion Matrix of the proposed IDS



	KDD CUP99	NSLKDD	UNSW NB15
Normal	0,98	0,99	0,935
Attacks	0,978	0,99	0,958

Figure 10. Classification Accuracy (ACC)



	GCC	CNN-AE	CNN	LSTM	SVMs	DBN
ACC	98,93%	93,44%	97,02%	94,21%	89,48%	85,77%
DR	98,76%	77,59%	97,04%	78,07%	95,18%	98,20%
FPR	0,75%	6,82%	0,85%	0,18%	15,21%	30,02%

Figure 11. Performance comparison

Meterial	Description
Processor	Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz
RAM	16 GB
Operating System	Ubuntu 20.04 LTS

Table 6. Machine Performances

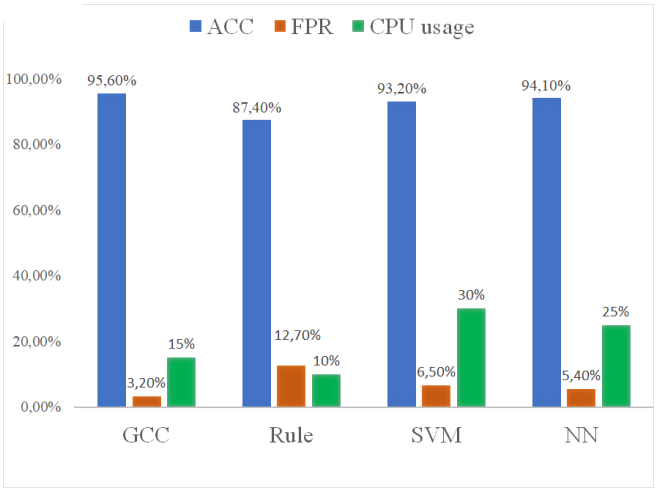


Figure 12. Comparative Analysis

IDS Model	Average Processing Time per Instance (seconds)
GCC-Based IDS	0.05
Rule-Based IDS	0.02
SVM-Based IDS	0.10
NN-Based IDS	0.08

Table 7. Average Processing Time

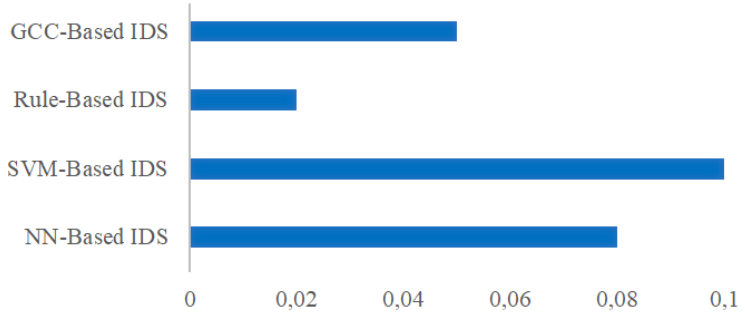


Figure 13. Average Processing Time

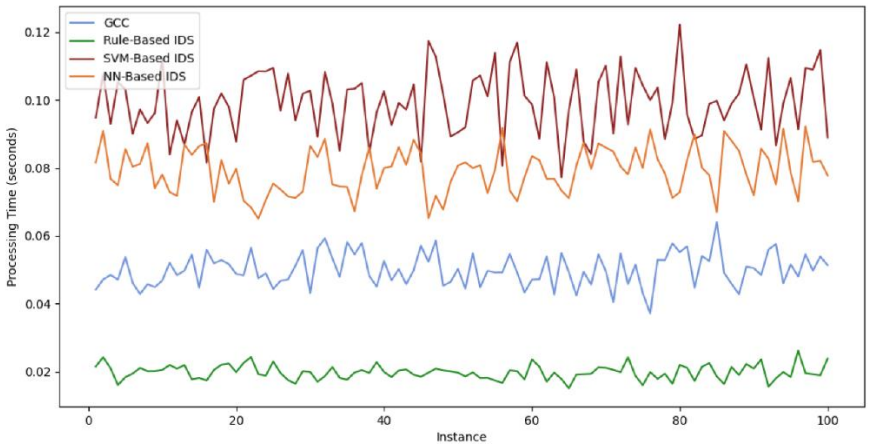


Figure 14. Processing Times for Different IDS Models Over Time

Biographies

Mekkaoui Kheireddine received his Bachelor's degree in Computer Engineering from the University of Sidi Bel Abbès in 2001, and his Master's degree in Computer Science from the University of Mascara in 2008. He earned his Ph.D. in Computer Science from the University of Sidi Bel Abbès in 2015. Currently, he is an associate professor and serves as a teacher and Research Chair at the University of Saida - Dr. Moulay Tahar since 2009. He collaborates with the IoT Lab at the University of Parma, Italy, and the LAMIA laboratory at the University of Trois-Rivières, Canada. He also contributes as a reviewer for various academic journals and international conferences. His research has been funded by the Ministry of Higher Education and Scientific Research. His research interests include security and privacy, malware analysis, artificial intelligence, and machine learning-assisted cybersecurity and their applications in technologies such as cloud computing, the IoT, big data, ad hoc networks, smart grids, and vehicular ad hoc networks (VANETs).

MEKOUR Mansour is an Assistant Professor at the University of Saida, Algeria. He received his PhD and M.S. degrees in computer science, specializing in Information and Knowledge Systems, from the University of Sidi Bel Abbes in 2014 and 2009, respectively. In 2005, he obtained a technical engineering degree in computer science, with a specialization in Artificial Intelligence, from the Computer Science Department of the University of Mascara, Algeria. His research interests include Service and Cloud Computing, Internet of Things and Smart Computing, Single and Multi-Objective Programming, Vehicle Routing and Scheduling Problem Solving, Machine and Deep Learning for Classification and Clustering.

TEGGAR Hamza received his Engineering degree in Computer Science in 2005 from the University Ahmed Ben Bella Oran 1, Algeria. He got the Magister degree in industrial informatics from University of Mascara in 2009 and the Phd degree in Computer science from Oran1 Ahmed ben Bella University in 2018. He is a Senior Lecturer at the University of Mascara, Algeria. He is also a research member of the Laboratory of Parallel and Embedded Architectures and Intensive Computing. His current research areas mainly focus on the application of artificial intelligence in the control of multi-robot systems and advanced control theory.