Ain Shams Engineering Journal 15 (2024) 102860

Contents lists available at ScienceDirect

Ain Shams Engineering Journal

journal homepage: www.sciencedirect.com

Full Length Article

Modeling time-varying wide-scale distributed denial of service attacks on electric vehicle charging Stations

Tawfiq Aljohani [a,*], Abdulaziz Almutairi [b]

[a] Department of Electrical Engineering, College of Engineering at Yanbu, Taibah University, Yanbu 41911, Saudi Arabia
[b] Department of Electrical Engineering, College of Engineering, Majmaah University, Almajmaah 11952, Saudi Arabia

ARTICLE INFO

Keywords:
DDoS attacks
Electric Vehicle Charging Stations (EVCS)
Cybersecurity of Energy Infrastructures
Cyberattacks Attack Generation Model
Ornstein-Uhlenbeck

ABSTRACT

With the continuous development of transportation electrification, Electric Vehicle Charging Stations (EVCS) have become pivotal components, necessitating robust cybersecurity frameworks to mitigate potential threats. This work explores the complex dynamics of Distributed Denial of Service (DDoS) attacks aimed at EVCS, highlighting the multifaceted interplay between the generation of attack traffic and its implications on grid stability. Introducing a novel mathematical model for extensive DDoS attacks on EVCS, this work simulates the attack methodology through a time-variant Poisson process, encapsulating the behaviors of attacks bots and their cumulative impact on the targeted EVCS. The model further incorporates the variability of attack intensity, utilizing the Ornstein-Uhlenbeck process to reflect on the temporal evolution and traceability of the attacks. Moreover, by integrating queueing theory, the model facilitates a detailed examination of traffic dynamics under DDoS conditions, providing insights into potential delays and service interruptions. The study also investigates the impact of DDoS attacks on both the dynamic and steady-state operation of the grid, offering a comprehensive perspective on the cybersecurity threat landscape. Simulation outcomes confirm that successful disruptions in EVCS due to DDoS attacks can lead to significant disturbances, underscoring the need for robust cybersecurity protocols.

1. Introduction

The transition towards transportation electrification is central in the global efforts to mitigate climate change and reduce greenhouse gas (GHG) emissions. At the forefront of this movement, Electric Vehicles (EVs) are poised to play a significant role in reducing emissions. However, their widespread adoption introduces complex and novel challenges in cyber-physical security, including their potential utilization as attack surfaces to infiltrate and compromise energy networks. These threats may not only have extensive implications for the stability of energy infrastructures, but also present significant risks to the safety of EV owners.

As smart grid technologies proliferate, there arises an imperative to establish expansive communication networks, thereby increasing potential security vulnerabilities associated with reliance on digital systems. The smart grid aims to create a self-regulating energy network with numerous interconnected components capable of bidirectional communication [1]. Such systems strive to achieve advanced grid infrastructure that promote optimal energy usage and management, ensuring reliable, cost-effective, and scalable energy solutions. However, this futuristic view of the grid faces significant challenges, as the smart grid's dependency on extensive networking and data exchanges exposes it to cyberthreats. Even minor security breaches can lead to severe consequences for smart grid components, putting consumers at risk [2]. Additionally, incorporating millions of EVs into power grids amplifies these cybersecurity risks. These vehicles could be leveraged as novel vectors for attacks, significantly endangering the smart grid's security. Such vulnerabilities could be exploited for political, social, or military objectives [3,4].

In contrast to internal combustion vehicles (ICVs), EVs exhibit unique challenges within the realm of cyber-physical systems as interconnected devices. Despite its increasing prominence, the domain of EV cybersecurity remains substantially uncharted, with considerable progress yet to be achieved. Recent years have witnessed a heightened awareness of the potential severe consequences for both vehicle operators and service providers, thereby placing the cybersecurity of EVs into spotlight. Attacks not only risk personal privacy and safety but also pose threats to the stability of the energy grid, questioning the sustainability

* Corresponding author.
E-mail addresses: torwi@taibahu.edu.sa (T. Aljohani), ad.almutiri@mu.edu.sa (A. Almutairi).

https://doi.org/10.1016/j.asej.2024.102860
Received 26 February 2024; Received in revised form 25 April 2024; Accepted 6 May 2024
Available online 22 May 2024
2090-4479/© 2024 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Engineering, Ain Shams University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

and reliability of EV technology. Consequently, robust cybersecurity protocols have become essential for the broader acceptance of EVs. Cyberattacks can inflict considerable economic damages, manipulate energy resources, and precipitate data breaches, potentially jeopardizing lives and eroding public confidence in the EV technology. Therefore, it is crucial to develop a secure and resilient EV infrastructure that can effectively detect and counteract cyberthreats.

As the EVs market continue to grow, a diverse set of stakeholders including energy providers, automotive manufacturers, end-users (EV owners), governmental agencies, and grid administrators becomes increasingly engaged in the EV marketplace. Accordingly, Electric Vehicle Charging Stations (EVCS) are recognized as critical infrastructures that necessitate enhanced protective measures against cyberthreats to facilitate their effective integration and functionality within the expansive EV ecosystem. The accelerated integration of EVs into local energy grids mandates the development of robust cyber-physical systems, ensuring secure and reliable bidirectional communication pathways. Specifically, the rapid incorporation of EVs increases their vulnerability to cyberattacks, potentially affecting all related stakeholders, driven by a range of motives. The potential for Distributed Denial of Service (DDoS) attacks poses a significant concern, as these could specifically target EVCS, disrupting their operation and compromising the stability of the broader grid infrastructure. This emergent risk of cyber intrusions demands comprehensive investigative efforts, aimed at ensuring the secure and seamless integration and operation of EVs across multiple dimensions. Therefore, this work presents an in-depth exploration of the cybersecurity of EVCS by discussing vulnerabilities due to DDoS attacks. In addition, the major contribution of this work, that was never reported in literature to the best of our knowledge, include the following:

1. A detailed mathematical model is presented, capturing the intricate behavior of DDoS attacks, their unpredictable nature, and the collective influence of botnets over EVCS.
2. By incorporating a time-variant Poisson process along with the Ornstein-Uhlenbeck process, the paper illustrates the variability in attack intensity and sheds light on the attack's progression and tracking over time against EVCS.
3. The utilization of queueing theory within this work contributes a novel discussion of traffic dynamics under DDoS attack conditions, helping to understand potential disruptions and delays in service, which is crucial for planning mitigation of similar cyberthreats.
4. The study examines the impacts of DDoS attacks on critical grid parameters such as active and reactive power, voltage, current, frequency levels, and generator's performance providing a hint on the implications of DDoS attacks on the dynamic and steady-state operation of the grid. In uncovering the complex mechanisms of these attacks and their potential effects on EVCS and grid stability, this work aims to foster a more secure and resilient smart grid environment.

2. DDoS threats on the landscape of electric vehicle charging stations

EVCS acts as an interface enabling EVs to charge or discharge energy into the power grids. Given their composition of both cyber and physical components, EVCS are susceptible to cyberattacks [5]. Such attacks might manifest as follows: an EV connected to a standalone or grid-integrated EVCS could become compromised. Once under cyber control, this scenario poses multiple security risks:

1. The compromised EV may allow the hacker to access the local power grid or hold the EV hostage, manipulating its various functionalities.
2. The hacker might interfere with the EV's charging process, potentially causing outcomes like equipment failure, thermal runaway, or manipulation of energy demands.
3. The attacker could disrupt the EV's charging or discharging operations via a Denial of Service (DoS) attack, potentially inducing instability in the local grid, particularly if many EVs are affected concurrently.

The physical layer of EVCS includes devices such as protection equipment, controllers, sensors, as well as vehicle charging communication devices like power line communication (PLC), advanced metering infrastructure (AMI) devices, and power electronics circuits. While generally protected from cyberthreats, the cyber layer—which manages these physical components via communication links—is highly susceptible to cyberattacks. Such attacks can inflict severe damage on the physical components. The connections that integrate the EV with the power grid through the EVCS include elements like communication links, internet service portals, in-vehicle electronics, on-board charging controllers (OBC), conventional power factor correction (PFC) circuits, human–machine interfaces (HMIs), radio interference devices, and original equipment manufacturers (OEMs). Hackers often target the EVCS with the goal of disrupting the efficiency of the charging/discharging process or causing substantial damage to the system components. Fig. 1 illustrates a typical EVCS system architecture, depicting the interconnection of the physical and cyber layers at the station.

EVCS plays a significant role in the rapid electrification of transportation systems and is central, at the same time, to maintaining proper balance between supply and demand within modern power grids [6]. Cyberattacks targeting these systems have the potential to disrupt this balance through the manipulation of charging and discharging processes [7]. Such disruptions can lead to unpredictable power demand fluctuations, causing grid instability or even widespread blackouts. The ramifications of these disturbances are profound, extending beyond the local environment of the EVCS to potentially affect the broader grid infrastructure. Furthermore, the efficiency and economic viability of EVs are significantly compromised by cyberattacks on EVCS. Interruptions or alterations in the charging schedules of EVs induced by cyberattacks can result in inefficient grid utilization. This inefficiency not only burdens the grid during peak demand periods but also leads to under-utilization during off-peak times. The economic impact of such inefficiency encompasses increased operational costs, potential revenue losses, and the accelerated degradation of infrastructure components, culminating in increased energy costs for end-users. Additionally, the security of the grid's communication networks, which facilitate the interconnection between EVCS and the grid, is pivotal. These networks transmit critical operational and management data, and their breach can lead to unauthorized access to grid controls and sensitive information. The implications of such breaches are far-reaching, potentially enabling large-scale manipulation of grid operations or data theft, posing a significant security threat.

The efficacy of DDoS attacks, as evidenced in their application against EVCS and broader smart grid infrastructure, can be attributed to their inherently distributed and sophisticated nature. This characteristic significantly complicates the task of combating and tracing these cyberthreats [8]. In comparison to other forms of cyber aggression such as False Data Injection (FDI), the selection of DDoS attacks as the focal point for this study is due to their direct and considerable impact on the operability of EVCS. The overwhelming traffic produced by DDoS attacks leads to observable disruptions, in contrast to the subtle manipulation's characteristic of FDI. Moreover, the accessibility and exploitation of communication channels by DDoS attacks underscore their relevancy and the challenge they pose in detection and mitigation efforts. Thus, the study prioritizes DDoS attacks, whose diversified and complex methods like jamming, flooding, de-synchronization, and amplification, offer a broad spectrum of challenges for cybersecurity defenses within the EVCS infrastructure. A key characteristic of these attacks is the utilization of spoofed IP addresses, a method that effectively conceals the attackers' identities. This approach to obfuscation greatly impedes efforts to trace the origins of DDoS attacks, a necessary

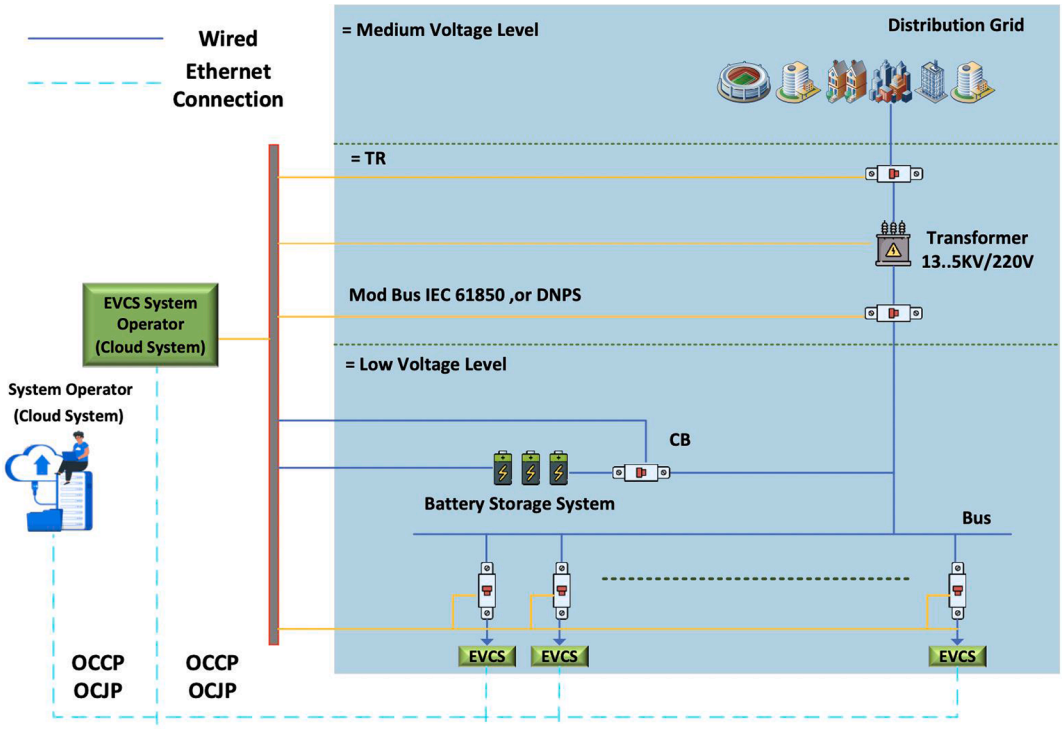


Fig. 1. Physical and cyber layer connections involved with typical EVCS.

step in both understanding and mitigating the threat. Within the context of EVCS, accurate source tracing is crucial for the security of the charging infrastructure, which is essential to the operational continuity and resilience of the smart grid. Furthermore, DDoS attacks exploit existing vulnerabilities within internet-connected hosts, targeting weaknesses not only in traditional network layers but increasingly in application layers as well. This trend towards targeting higher-level protocols and software components is particularly alarming for systems like EVCS, which depend on sophisticated software interfaces and communication protocols for grid synchronization and operational management.

In addressing DDoS attacks, a thorough comprehension of their dimensions is critical. This includes an understanding of attack typologies, methodologies, and potential points of exploitation. Research literature over the past decade, including studies in [9–12], has yielded extensive classifications and analyses of DDoS attacks, demonstrating the evolving and complex nature of these cybersecurity challenges. From a technical perspective, counteracting DDoS threats within the context of EVCS and smart grids requires a multi-faceted approach. This approach should incorporate advanced detection algorithms, robust mitigation strategies, and the development of resilient system architectures. It also necessitates the continuous evolution of cybersecurity measures to preempt and adapt to the dynamic landscape of cyberthreats. Guaranteeing the security and reliability of EVCS against such sophisticated attacks is imperative not only for the immediate protection of these systems but also for the broader stability and sustainability of smart grid technologies [13].

A recent development in the realm of DDoS attacks within wireless networks involves the disruption of communication at the physical layer, specifically targeting smart grid devices. This disruption is achieved through signal jamming, a technique that varies in complexity from continuous interference transmission to more sophisticated methods exploiting application layer protocol vulnerabilities [10,14]. The authors in [15] orchestrated a jamming attack aimed at two objectives: disrupting electrical service within a specified timeframe and inducing physical disturbances in the power grid frequency, leading to load shedding. Other studies such as in [16,17] investigated both jamming and countermeasures in a multichannel wireless network linking remote sensors to a smart grid's control center. The interaction between the grid sensors and the attacker was modelled as a zero-sum stochastic game, highlighting the strategic nature of these attacks and defenses. When it comes to EVCS, these DDoS-based jamming attacks present a significant threat. They could potentially disrupt the communication between EVCS and the control systems of the smart grid, leading to charging delays or even complete service denials. This disruption is not just a matter of inconvenience; it could have broader implications for grid stability, especially if timed to coincide with peak demand periods. To detect and mitigate such jamming attacks in the context of EVCS, techniques often focus on analyzing network signal stability parameters, like signal strength indicators and packet loss rates [18]. Other strategies include consistency monitoring, delayed disconnects, and observing of the media access control layer for signs of misbehavior. Additionally, intelligent channel selection can be employed to avoid channels under attack, enhancing the resilience of EVCS communication networks against such disruptions [19]. These strategies are significant in maintaining the operational integrity of EVCS within the smart grid, ensuring that EVs can be charged reliably without jeopardizing the stability of the entire distribution system.

Building on the discussion of jamming attacks and their implications for EVCS, another prevalent type of DoS cyberthreat is the flooding attack. This type of attack aims to overwhelm the network, leading to delayed or completely interrupted communications between legitimate devices within the smart grid, including EVCS. Such attacks exploit various network protocols, namely Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), or Transmission Control Protocol (TCP), to generate significant disruptions. Despite their simplicity in execution, the impact on network functionality can be substantial. TCP SYN Flooding, for instance, utilizes the TCP/IP protocol's three-way handshake mechanism, which is susceptible to exploitation by many smart grid protocols, including those used by EVCS like Modbus TCP [20]. In this type of attack, the perpetrator sends a SYN request packet to the EVCS, which responds with an SYN/ACK packet and awaits a

concluding ACK packet to establish the connection. However, by omitting the ACK packet, the attacker forces the EVCS to keep the port open indefinitely, eventually depleting its capacity to initiate new connections with legitimate devices. This form of attack can cripple the operational capabilities of EVCS, leading to significant delays in charging processes and potentially impacting broader grid functionality. Similarly, UDP Flooding attacks involve targeting the EVCS with a high volume of packets directed at random ports. As highlighted in [21], such attacks can have devastating effects, potentially leading to wide-spread blackouts in the energy infrastructure. If the EVCS cannot communicate effectively with the control center, this might lead to a failure in managing power distribution demand, resulting in widespread grid instability.

Ping flooding, another DoS variant, overloads the network with ICMP Echo Request (ping) packets [22,23]. This attack utilizes the entire bandwidth available to the victim, in this case, the EVCS, hindering it from processing legitimate communications. Depending on the EVCS's role in the smart grid, such an attack could have varying physical consequences, from delayed critical messages to complete service disruption. To mitigate these flooding attacks, deploying network Intrusion Detection Systems (IDS) and anomaly detection is crucial [24–27]. These IDS systems are designed to monitor network traffic for signs of unusual activity, facilitating a rapid response to potential threats. Additionally, advanced moving target defense mechanisms, as outlined in [25], can be employed to dynamically alter network configurations, making it increasingly difficult for attackers to exploit such vulnerabilities. In the context of EVCS, the implications of flooding attacks are profound. As EVCS are pivotal in balancing energy demand and supply within the future smart grid, any disruption to their operation can have cascading effects on the stability and efficiency of the entire grid. Therefore, ensuring robust cybersecurity measures for EVCS against such attacks is not only essential for the reliability of EVs charging infrastructure but also for the overall resilience of the smart grid.

Continuing the exploration of cybersecurity threats to EVCS, a further critical concern emerges from DDoS-like de-synchronization attacks. These attacks are particularly insidious due to their capacity to disrupt the exact timing necessary for numerous smart grid applications, essential for the operation of EVCS. Such applications often rely on synchronous measurements that necessitate precise timing information. GPS signal spoofing is a prevalent method utilized to execute de-synchronization attacks within the smart grid. Most measurement equipment, critical to the operation of EVCS, depends on GPS to secure accurate timing. These devices regularly sample attributes such as frequency and voltage, aligning these measurements to a common time domain managed by the control center. The authors in [28,29] explore the impact of de-synchronization attacks on smart grid applications, including transmission line fault detection, voltage stability monitoring, and event localization. They illustrate how time de-synchronization attacks can compromise these applications, leading to faulty operations within the smart grid. Moreover, these attacks can be executed by exploiting vulnerabilities in the Precision Time Protocol (PTP), as detailed in IEEE 1588 protocols. This protocol, crucial for time synchronization among devices with disparate clock resolutions, is extensively utilized in smart grids at the substation level for microsecond-accuracy measurements. The PTP master, deriving its timing from GPS signals, is susceptible to several types of attacks, including DoS, packet manipulation, and selective packet delay [30]. An attack that introduces delays in the PTP master communication pathway can significantly disrupt the timing of connected devices, impacting essential functionalities such as fault localization and differential protection. For EVCS, the ramifications of such de-synchronization attacks are considerable. As these stations increasingly depend on precise timing for effective energy management and grid integration, any disruption can lead to charging inefficiencies, potential energy wastage, and may even jeopardize the stability of the local grid. To counteract de-synchronization threats, several strategies have been developed. Monitoring the GPS carrier-to-noise ratio across different layers is an effective technique to detect time de-synchronization attacks [31,32]. Additionally, utilizing highly stable atomic clocks or adhering to the IEEE 1588–2008-time synchronization protocols provide a layer of protection [33]. The implementation of authentication mechanisms to counter spoofing attacks, which are often the primary facilitators of de-synchronization, is also crucial. Ultimately, protecting EVCS from de-synchronization attacks is important for the reliable and efficient operation of the smart grid. As the grid progresses with increasing reliance on precise timing for various functionalities, the significance of effective defense and mitigation techniques against such cyber threats escalates. These measures are critical not merely for the security of individual EVCS but for the overall stability of the smart grid infrastructure.

Amplification attacks are yet powerful type of DDoS attack that threatens the stability and functionality of EVCS. These attacks exploit network traffic reflection and amplification, overwhelming targeted systems with minimal effort from the attacker. In these scenarios, the perpetrator spoofs an IP address (reflection) and utilizes UDP-based protocols that generate a much larger response than the attacker's initial request (amplification), overwhelming the network [34]. Unlike traditional flooding attacks, amplification attacks are more resource-efficient for attackers although more complex to implement. They exhibit four main characteristics [35]:

- Distributed Nature: Utilizes multiple servers with UDP protocol.
- Concealment: Attackers hide their identities by spoofing IP addresses.
- Indirect Impact: Traffic reaches the victim indirectly via reflected amplification.
- Increased Load: Traffic directed to the victims is significantly amplified.

Within the EVCS landscape, common forms of amplification attacks include Domain Name System (DNS), Network Time Protocol (NTP), and Simple Network Management Protocol (SNMP) amplification. For example, DNS amplification involves sending UDP packets with forged IP addresses to DNS resolvers that act as amplifiers, leading to service interruptions by flooding the network with excessive responses [36]. Similarly, NTP amplification employs NTP servers to excessively overload network communications [37].

Amplification attacks on EVCS present severe risks due to their reliance on stable network connections for operational efficiency and grid synchronization. Such attacks could profoundly disrupt these connections, resulting in charging delays, potential data loss, or even temporary cessation of charging capabilities. To counteract these threats, Yang et al. [38] propose an intrusion detection system specifically designed for synchrophasor measurements in smart grids. This system incorporates protocol-based whitelists with behavioral anomaly detection and deep packet inspection to effectively counteract both man-in-the-middle and amplification attacks. The objective of such defense mechanisms, similar to those implemented against flooding attacks, is to prevent the saturation of network bandwidth or the overload of devices processing network packets. Ultimately, amplification attacks pose a critical cybersecurity challenge for EVCS. Their capacity to disrupt network operations necessitates the deployment of sophisticated defense and mitigation strategies. Ensuring the resilience of EVCS against such attacks is imperative for maintaining the reliability and efficiency of EVCS and, by extension, the stability of the smart grid system.

To bridge the clear research gap in this emerging topic, Section 3 of this manuscript presents the proposed mathematical model, designed to simulate the dynamics of DDoS attacks on EVCS. Employing a time-variant Poisson process and integrating queueing theory, this model provides a robust framework to comprehend and identify these cyber threats for a safer and reliable operation of EVCS.

3. Proposed mathematical model of the DDoS attack generation on EVCS

Given their unique consumption patterns, EVs could be utilized as novel attack vectors against the distribution grids. The unique consumption patterns of EVs provide opportunities for malicious activities that were previously considered unviable. Notably, even minor fluctuations in the EV charging loads can lead to disproportionately large disturbances in the grid if not isolated in a timely manner. Additionally, given the inherent properties of power flow, there is a possibility for the frequency to undergo rapid increases or decreases due to sudden load changes. Also, maintaining voltage within a specified range, commonly ±8% of the nominal value, is crucial due to its direct correlation with the reactive power of the system. Moreover, due to the non-linear characteristics inherent in battery charging dynamics, a surge in reactive power demand from EV loads may result in notable voltage oscillations. DDoS attacks on EVCS, by disrupting communication and control processes, can intensify these issues, potentially destabilizing both dynamic responses and steady-state conditions of the power grid.

This work introduces a stochastic model for simulating DDoS attacks on EVCS servers, utilizing the Poisson distribution as the core statistical framework. The objective is to ensure uninterrupted server operations by precisely identifying attack patterns within defined time intervals. Key assumptions include that DDoS attacks make EVCS servers unavailable, and that these servers are equipped with Intrusion Detection Systems (IDS). This study set forth that attack occurrences are random, adhering to a Poisson distribution that captures the discrete event nature of network traffic. The model further assumes that the probability of server malfunction due to DDoS attacks is quantifiable and adheres to a specific distribution. It integrates a proactive monitoring policy, focusing on discrete packet count changes over time to detect attacks. Once an attack is detected, the server temporarily suspends client services to trace and mitigate the attack, restoring normal operations upon neutralizing the threat.

The rate at which each bot generates attack requests is modeled as a dynamic process over time, described as a time-varying Poisson process denoted by $\lambda(t)$. Within this framework, λ_{base} represents the foundational attack rate, while $\lambda_{var}(t)$ represents the evolving variations in attack intensity as time progresses, as follows:

$$\lambda(t) = \lambda_{base} + \lambda_{var}(t) \tag{1}$$

$$T(t) = N.\int_0^t \lambda(s)ds \tag{2}$$

Here, $\lambda(s)$ denotes the rate at which individual bots within the botnet generate attack requests at time s, while N represents the total number of active bots impacting the compromised servers in the EVCS. The transition matrix, Q_{ij}, is employed to characterize the dynamic transitions of bots across various operational states. To clarify, considering i as the count of active bots at a particular moment and j as the count following a transition, the matrix Q_{ij} is formulated as follows:

$$Q_{ii}(t) = -\lambda_i(t) \tag{3}$$

$$Q_{ij}(t) = \lambda_i(t).P_{ij}(t) \tag{4}$$

When i=j, the transition rate is $-\lambda_i(t)$, signifying that there is no change in the number of active bots. On the other hand, when the transition rate is positive, this indicates that the bots may change their states with $P_{ij}(t)$ representing the probability of changing the state from i to j. Moreover, the probability distribution of the number of attack bots follows a Poisson distribution, which could be defined by the cumulative attack rate:

$$P(X(t+\Delta t) = i|X(t) = j) = \text{Poisson}(i, \lambda(t)).\Delta t \tag{5}$$

The probability of observing k attacks in a time interval [0, k] is given by:

$$P(X(t) = k) = \frac{e^{-\Lambda(t)}.\Lambda(t)^k}{k!} \tag{6}$$

$$\Lambda(t) = \int_0^t \lambda(u)du \tag{7}$$

where $\Lambda(t)$ represents the cumulative intensity function. The evolution of the attack rate for each bot is modeled as a stochastic process following the Ornstein-Uhlenbeck [39], as follows:

$$d\lambda_{var}(t) = -\alpha\lambda_{var}(t)dt + \sigma dW(t) \tag{8}$$

where α denotes the mean-reversion rate; σ denotes the volatility; and $dW(t)$ represents the Wiener process that is used to reflect on the queue length, accounting for random variations in arrival and service processes. The expected value of the Wiener process increment equals zero, while its variance is proportional to the time increment dt, as follows:

$$E[dW(t)] = 0 \tag{9}$$

$$E\left[(dW(t))^2\right] = dt \tag{10}$$

The size of each attack request can be modeled as log-normal distribution, with the traffic received at the EVCS represented as follows:

$$Attach - Size(t) \sim LogNormal(\mu, \sigma^2) \tag{11}$$

$$X_{received}(t) = \int_0^t X(s).Attack\_Size(s)ds \tag{12}$$

Queueing theory [40] is applied to manage the EVCS traffic during a DDoS attack. The M/G/1 queue model, featuring time-varying arrival rates and service rates, offers insights into the dynamic nature of incoming requests and their processing times. The queue length, essential for understanding potential delays during attacks, is described within the framework of stochastic fluctuations and random variations in system processes, illustrated as follows:

$$dQ(t) = [\lambda(t) - \mu(t)]dt + dW(t) \tag{13}$$

Equations (13) models potential variations due to the DDoS attack, here $Q(t)$ represents the queue length at the EVCS that captures the number of incoming requests that are waiting to be processed at time s, which is evolved based on the difference between $\lambda(t)$ and the service rate $\mu(t)$. The service rate is an inversely proportional function of the capacity of charging ports of the EVCS. During a DDoS attack, if the attack disrupts the availability of some of those charging points, it can directly impact the service rate, as follows:

$$\mu(t) = \frac{C}{R_{active}(t)} \tag{14}$$

Upon detecting a DDoS attack, the server system immediately interrupts charging services to initiate a comprehensive trace of the intrusion. This trace, if successful, leads to the termination of the attack, and subsequently, the server system restores its operational state and resumes charging requests, thereby ensuring continuity and security post-attack resolution. The server's return to service post-attack is modeled by a Beta distribution, $B(t; \alpha(t), \beta(t))$, with time-varying shape parameters representing the distribution of the server's recovery time. However, failure to trace attacks triggers a complex refreshment process, modeled by a distribution $G(t)$, with a variable mean $1/G(t)$. This process incorporates a secondary Poisson model to simulate the likelihood of server recovery or failure during refreshment, providing a comprehensive view of server resilience in the face of sustained attack.

Here, this work utilizes a non-homogeneous Markov process to model the EVCS server's refreshment process. The state transitions (from processing to refreshment, and from refreshment to either recovery or failure) are governed by time-dependent transition rates. The transition rate from refreshment to recovery, $\mu_r(t)$, and from refreshment to failure, $\mu_f(t)$, both vary over time. The transition probabilities over a small interval δt are given as follows:

$$P_{r\to f}(t, t+\delta t) = \mu_f(t)\delta t + o(\delta t) \tag{15}$$

$$P_{f\to r}(t, t+\delta t) = \mu_r(t)\delta t + o(\delta t) \tag{16}$$

where r, f, and s represent refreshment, failure, and successful recovery states, respectively. In the context of DDoS attacks, the modeling of the impact on EVCS needs to consider both steady-state and dynamic conditions of the grid. Steady-state models focus on long-term system behavior without transient effects, typically examining how persistent changes in demand affect voltage and frequency stability. Dynamic models, conversely, investigates the transient behaviors during and immediately after disturbances, essential for assessing the resilience of grid operations during fluctuating DDoS conditions. Hence, a successful launch of series of DDoS attack can affect the active and reactive power demand at the EVCS, as follows:

$$P_{EVCS}(t) = P_{nominal} - \Delta P_{attack}(t) \tag{17}$$

$$Q_{EVCS}(t) = Q_{nominal} - \Delta Q_{attack}(t) \tag{18}$$

where $P_{nominal} and Q_{nominal}$ represents the nominal active and reactive power of the EVCS while $\Delta P_{attack}(t)$ and $\Delta Q_{attack}(t)$ represents the change of active and reactive power due to the DDoS attack. The active and reactive power impact can be further modeled based on the attack intensity and duration, considering the load profile and power distribution characteristics:

$$\Delta P_{attack}(t) = P_{load}(t) - P_{supply}(t) - P_{loss}(t \tag{19}$$

$$\Delta Q_{attack}(t) = Q_{load}(t) - Q_{supply}(t) \tag{20}$$

Voltage and frequency deviations is highly expected to witness major variations due to the DDoS attack on EVCS and other grid-connected devices, as follows:

$$\Delta V_{ch}(t) = V_{nominal} - V_{ch}(t) \tag{21}$$

$$\Delta f_{grid}(t) = \frac{1}{2\pi}\left(\frac{\Delta P_{attack}(t)}{M} - \frac{\Delta Q_{attack}(t)}{D}\right) \tag{22}$$

where $\Delta V_{ch}(t)$ represents the deviation of the charging voltage levels, which is the difference between the nominal per unit voltage $V_{nominal}$ and the voltage during the time of the attack t. On the other hand, M and D represents the grid's inertia constant and damping factor, which are important to quantify potential deviations in frequency levels. Also, such modeling must consider the operational constraints in distribution systems, as follows:

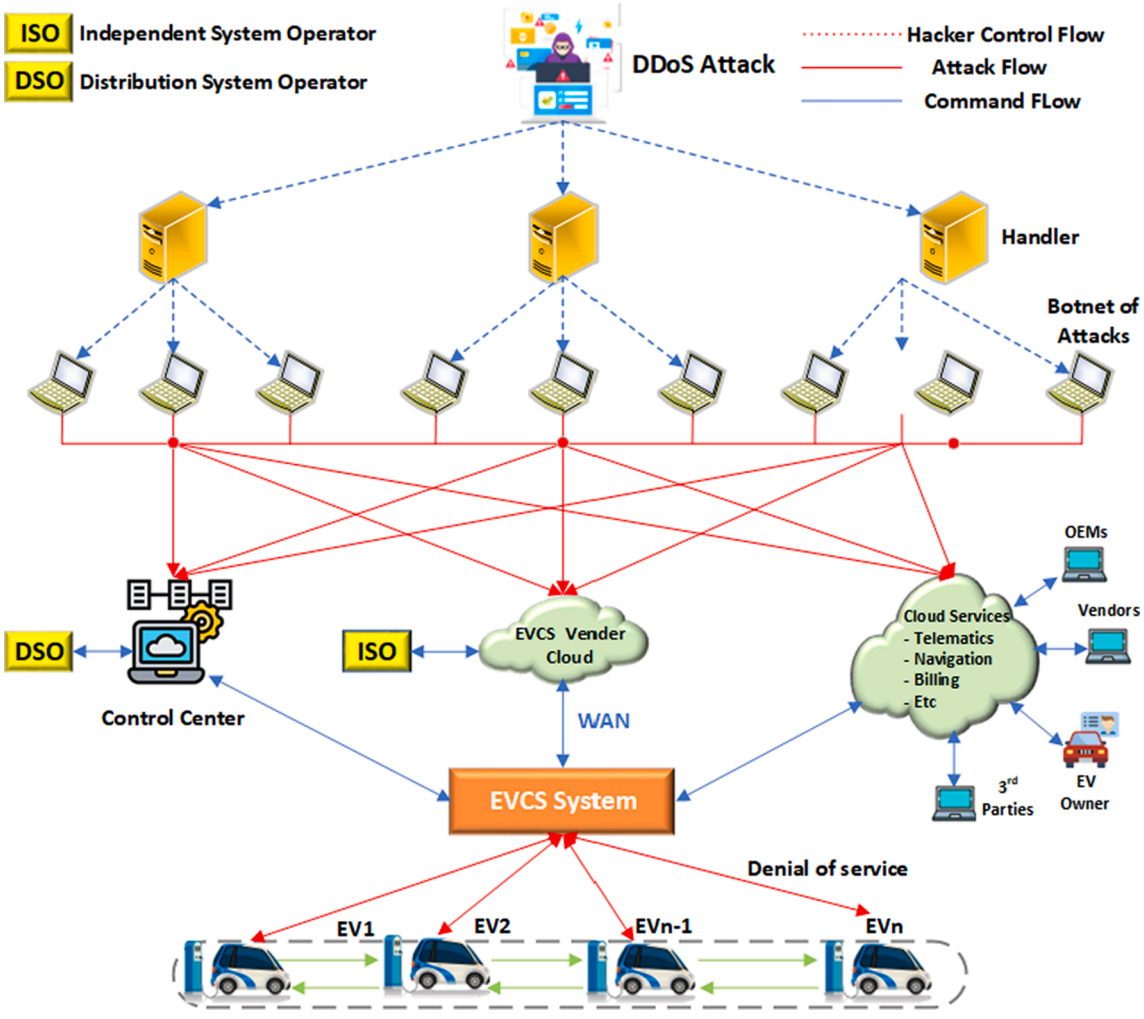


Fig. 2. An illustration of performing DDoS attacks on EVCS as performed in the case studies.

$$P_{min} \leq P_{EVCS}(t) \leq P_{max} \quad (23)$$

$$Q_{min} \leq Q_{EVCS}(t) \leq Q_{max} \quad (24)$$

$$V_{min} \leq V(t) \leq V_{max} \quad (25)$$

Fig. 2 presents an illustration of the wide-scale DDoS attack against an EVCS as envisioned in this work.

4. Case studies and results

4.1. Test system and simulation environment

Table 1 offers a detailed view of the EVs charging demands across various penetration levels and charger capabilities. The penetration benchmarks, namely 10%, 18%, 25%, and 30%, are designed to assist utilities and policymakers in understanding the potential upsurge in electricity demand as EV adoption grows. Level 2 chargers, primarily operating within the 208–240 V range, are common in both residential and commercial settings. The 7.2 kW level is typical of standard home chargers, often found in residential areas, workplaces, and small microgrids systems. Similarly, the 11 kW and 19 kW chargers, noted for their higher capacities, are frequently utilized in commercial settings where Level 2 charging is essential. On the other hand, Level 3 or DC fast chargers, with designs that enable rapid charging, are suitable for public charging stations or fleet operations.

To explore the ramifications of the DDoS attacks on the EVCS, this study utilizes a modified IEEE 33-bus distribution test system, with proposed EVCS located at buses 13, 18, and 33, and a wind turbine of 2.6 MW output on bus 3, as illustrated in Fig. 3. The Python environment serves as the simulation tool in this work, where specific Python-based power system simulation libraries facilitate power flows, contingency analyses, and other relevant power system operations. The power factor associated with the EV charging process is defined as p.f. = 0.92 lagging. Data on the arrival and departure of EVs to the EVCS were sourced from references [41,42].

The Python-developed simulation model adeptly captures the complexities of DDoS attacks targeting the communication infrastructure of the modified IEEE 33-bus test system, with a particular focus on the EVCS servers. The integration of "*PyPSA*" and "*Pandapower*" in this study enables comprehensive modeling of the power grid's responsiveness to cyber disruptions. Notably, "PyPSA" plays a crucial role in simulating grid dynamics and power flow during attack scenarios, while "Pandapower" provides robust tools for contingency analysis and network configuration under simulated attack conditions. The results from the model deliver a detailed perspective on attack dynamics, unveiling the frequency, intensity, and success rates of the simulated attacks.

In this simulated context, DDoS attacks are conceptualized as stochastic processes designed to overload the EVCS's communication channels with an overwhelming volume of data packets. The attack pattern adheres to a Poisson distribution, ideally suited for modeling the occurrence of independent events within a set time frame. The parameter λ signifies the average number of attacks per unit time, allowing for the simulation of varied attack intensities. The communication

Table 1
Penetration levels of EVs in regular distribution feeder.

Penetration levels	10%	18%	25%	30%
Level 2 chargers				
7.2 kW	1,500	2,700	3,600	4,320
11 kW	2,100	3,780	5,250	6,300
19 kW	3,800	6,840	9,500	11,400
Level 3 chargers				
40 kW	8,500	15,300	21,250	25,500
240 kW	50,000	90,000	125,000	150,000

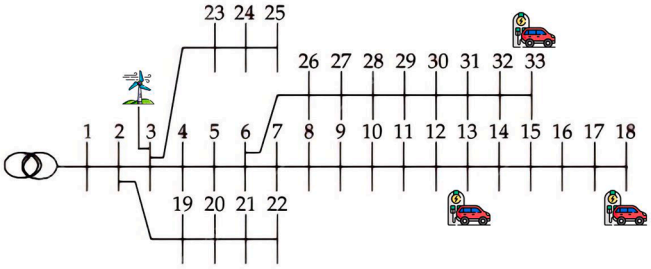


Fig. 3. Modified IEEE 33 test system with wind generator on bus 3 and EVCS on nodes 13, 18 and 33.

infrastructure within the EVCS is depicted as data pipelines, specifically designed to manage network traffic capacities. Under standard operating scenarios, these pipelines facilitate the transmission of control signals, status updates, and user requests. Python's handling of asynchronous I/O operations provides a realistic emulation of these pipelines, with the "*asyncio*" library proving essential for simulating communication link behavior in terms of capacity and latency both during normal operations and under attack conditions.

Data packets in the simulation are treated as distinct objects, each defined by attributes like size, source, and destination, reflecting real-world network traffic. These packets are generated at rates determined by the Poisson distribution, using the "*NumPy*" library for random sampling, resulting in a realistic modeling of both legitimate and malicious data traffic. This Poisson model is also employed to simulate the frequency of attack events, with the Python implementation utilizing the "*numpy.random.poisson*" function to determine the occurrence of attacks within each interval, consistent with the defined rate parameter λ. Furthermore, the duration of each attack, or the period during which the communication channel is overwhelmed, is modeled following a Poisson distribution, with μ denoting the mean duration of attacks. This model facet enables the exploration of both transient and prolonged attacks, shedding light on their respective influences on the EVCS. Fig. 4 showcases the outcomes of simulating random DDoS attacks on EVCS servers, where only two out of 52 attacks within a 1000-second interval successfully disrupted the servers by denying charging requests. Importantly, the instances of successful attacks highlighted in Fig. 4 reflect scenarios where the IDS were either momentarily overwhelmed or the attack signatures were sophisticated enough to bypass detection mechanisms. These rare successful attacks exemplify potential real-world situations where, despite robust security protocols, a residual risk of compromise persists. These anomalies within the attack distribution provide valuable insights for refining IDS algorithms and enhancing system defense protocols. By adopting the Ornstein-Uhlenbeck process to account for variability in attack intensity, this study recognizes the temporal correlations in attack rates that may induce periods of increased risk. During such high-risk phases, the IDS is required to function with enhanced sensitivity, which might be bypassed by a coincidentally well-timed and large-scale attack, as evidenced by the successful attacks depicted in Fig. 4.

4.2. Small-scale DDoS attack generation

To put it in context, this study initiates various adversarial DDoS attacks aimed at introducing load manipulations that induce significant frequency deviations within the grid. In this scenario, an incremental load of 3 MW, representative of 429 EVs each utilizing 7.2 kW level 2 chargers, was distributed across selected buses—13, 18, and 33—within the test system. Initially, DDoS attacks were strategically implemented at an EVCS located at bus 13, which supports 15% of the load on the distribution feeder. This involved orchestrating a denial of service to 12 charging ports at three specific times: $t_1 = 80$ s, $t_2 = 180$ s, $t_3 = 355$ s, as illustrated in Fig. 5. The duration of the attacks, prior to the activation of

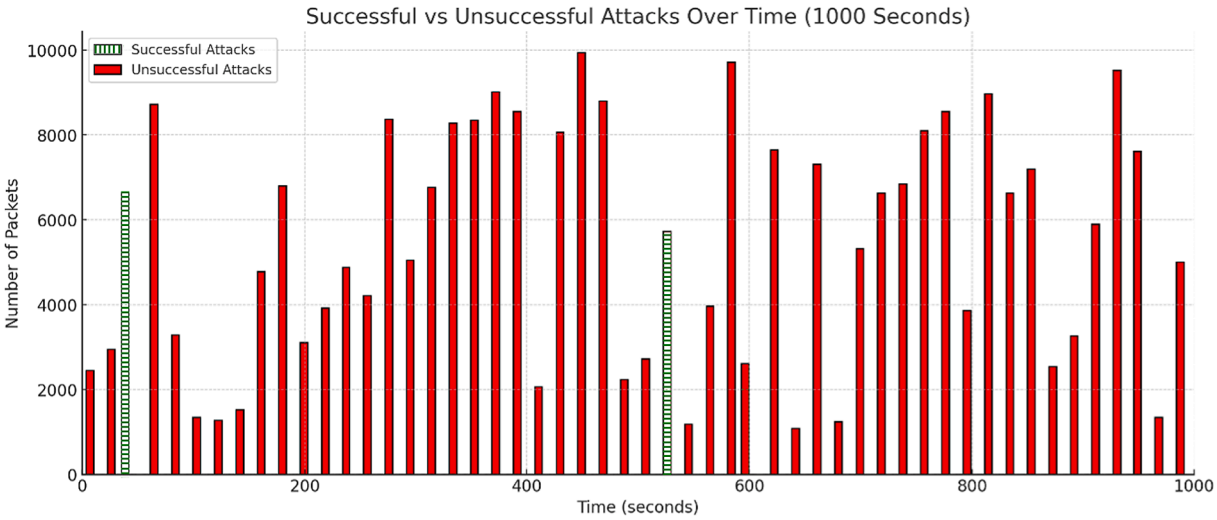


Fig. 4. Successful vs. unsuccessful DDoS attacks against EVCS.

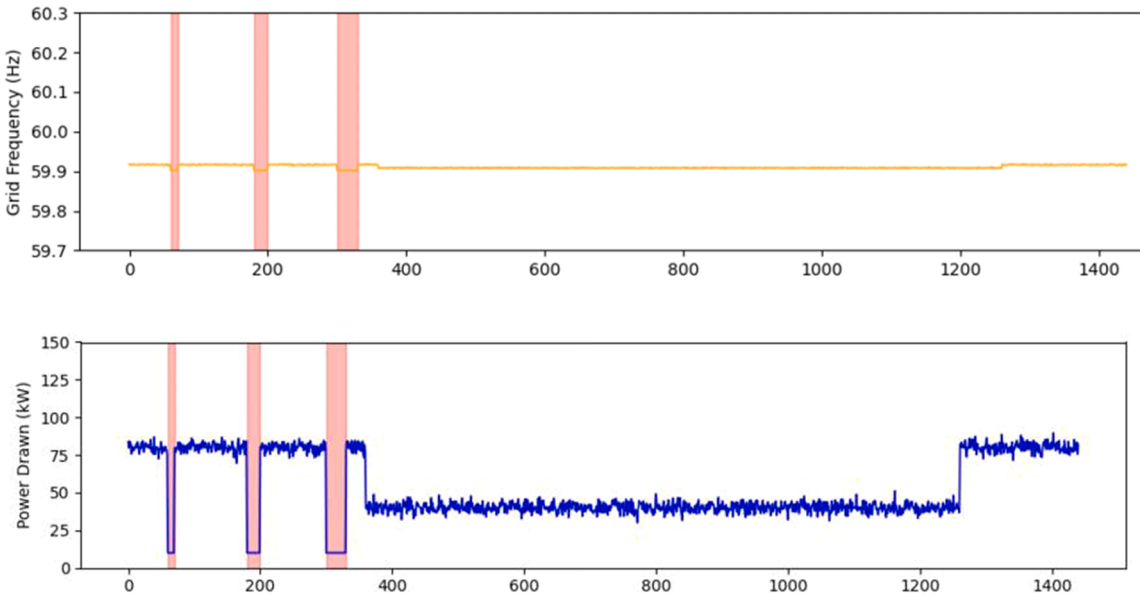


Fig. 5. Impact of a DDoS attack on 12 charging ports on frequency (above) and charging active power (down).

protective measures, lasted 10, 20, and 32 s respectively. Fig. 5 also highlights the impact of these attacks on the power output from the EVCS at bus 13, where a complete denial of service to 12 ports resulted in a very minor, almost negligible, frequency disturbances during the attack periods, primarily due to the limited scale of the attack. The observed fluctuations in active power, as illustrated by the lower part of Fig. 5, reveal the grid's vulnerability to even small-scale attacks, which can cause immediate disturbances in the dynamic response of the system. These oscillations emphasize the need for comprehensive dynamic modeling to capture and analyze the transient behaviors and interactions within the grid due to attacking bots, to devise proper mitigation strategies against cyber-induced instabilities, as thoroughly examined in the proposed mathematical formulations in this work.

In the event of escalating power demand due to large-scale attacks, a detectable reduction in generator output is foreseen, which could precipitate a noticeable drop in grid frequency. If such frequency drops exceed predefined operational thresholds, it could lead to a sequence of generator disconnections, further aggravating the frequency disturbances and raising the specter of a comprehensive blackout.

4.3. Large-scale DDoS attack generation

The exacerbation of the grid's vulnerability is observed predominantly during periods of peak demand when the operational margins are minimal. Grids with a substantial reliance on renewable energy sources are particularly at risk due to inherently lower levels of inertia, which compounds the grid's sensitivity to fluctuations. This study quantifies the magnitude of such disturbances by examining the outcomes of the two successful DDoS attacks that is aimed at the EVCS across buses 13, 18, and 33. Recorded at distinct instances—$t_1 = 55$ s and $t_2 = 510$ s—these attacks led to an equivalent active power load increase of 3.11 MW, similar to the concurrent charging of 429 EVs at a 7.2 kW rate with 96% charging efficiency. Through the application of the "*pyocpp*" library, a '*remote_stop_connection*' function was issued, effectively isolating the compromised IP addresses and precluding further unauthorized charging activity. Subsequent to these interventional measures, a marked reduction in active power consumption is noticed, as highlighted by Fig. 6. This decline in power draw, precipitated by the abrupt termination of charging processes, is most marked at the specifically targeted buses. Concurrently, the system experienced considerable

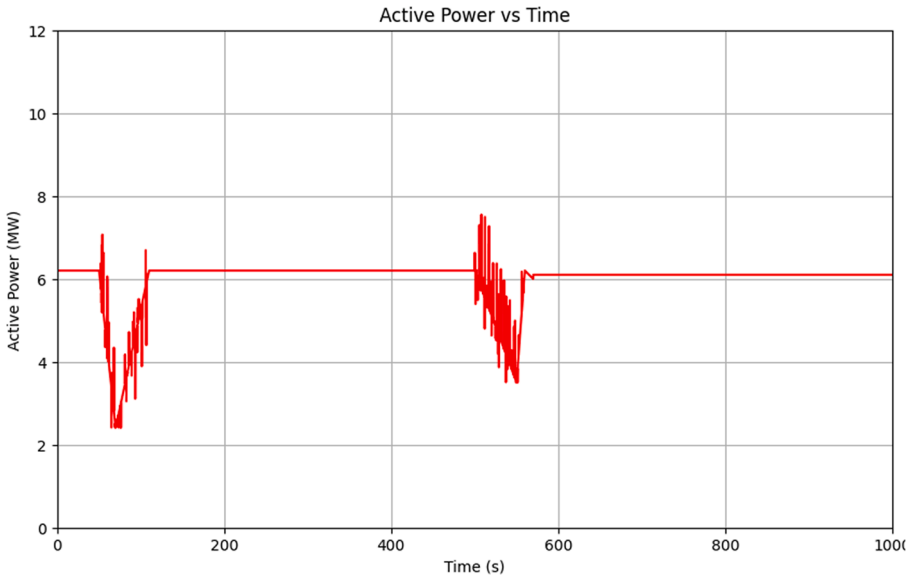


Fig. 6. Active power loss due to denial-of-service attacks.

variations in reactive power, as depicted in Fig. 7. These observed phenomena underscore the need of integrating sophisticated mathematical models that accurately reflect the grid's steady-state equilibrium and dynamic response to cyberattacks. The inherent characteristics of EV charging, which necessitates both active and reactive power, imply that any interruption affects not only real power but also impacts the reactive power domain, thus influencing the voltage profile across the affected buses. As illustrated in Fig. 8, the voltage profile at the test system exhibited an increase post the cyber events where a rise in voltage levels was an expected, yet worrisome, outcome. This is predictable as voltage levels are directly correlated with active power; when demand suddenly decreases without a corresponding reduction in generation, the system encounters a transient overvoltage.

Following the cyber interference, an increase in the system frequency was observed. Under normal operating conditions, the balance between generated power and load demand governs system frequency. The cyber-induced load reduction created an imbalance, with generation momentarily exceeding the reduced demand. This transient over-generation phenomenon was manifested as a frequency increase. The erratic frequency trajectory, coupled with voltage fluctuations as depicted in Fig. 9, exceeds established safe operational parameters. Such deviations pose risks of activating protective relays, potentially leading to extensive load shedding or even a full-scale blackout. These unpredictable fluctuations jeopardize the grid's stability, potentially triggering the system's protective relays and leading to a blackout. Furthermore, the fluctuating power demands impose rapid accelerative and decelerative forces on the generator's turbine/prime movers, exacerbating rotor vibrations. Such stress can cause permanent, costly damages. To mitigate these risks, ultra-sensitive protective relays are crucial, although their activation might result in blackouts and significant economic impacts.

Additionally, the wind turbine generator located at bus 3 displays transients, characterized by significant oscillations in power output, as illustrated in Fig. 10. The model depicts a rapid transient stabilization within the initial two seconds, followed by the generator's stabilization at a consistent nominal output level. This phase represents the

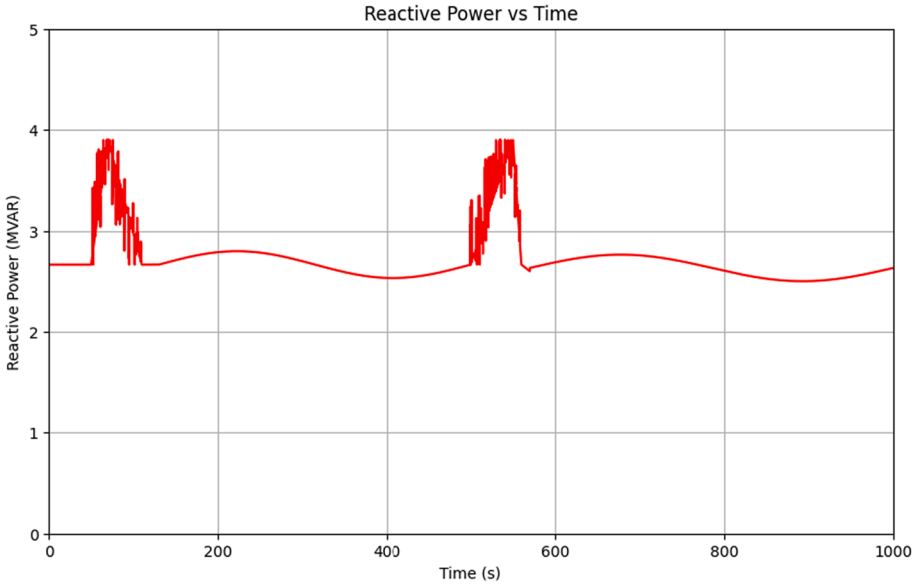


Fig. 7. Reactive power fluctuations due to denial-of-service attacks.

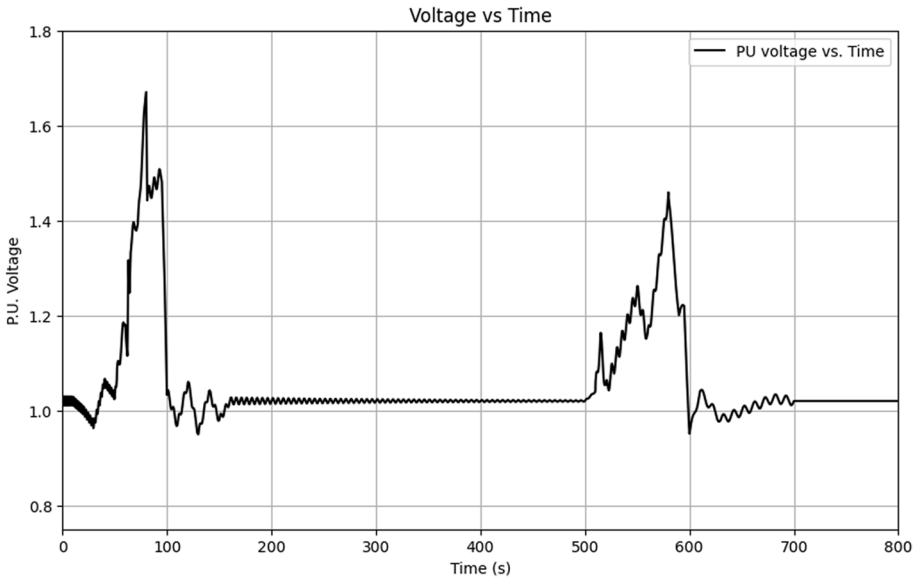


Fig. 8. Per unit voltage fluctuations due to attacks on buses 13, 18 and 33.

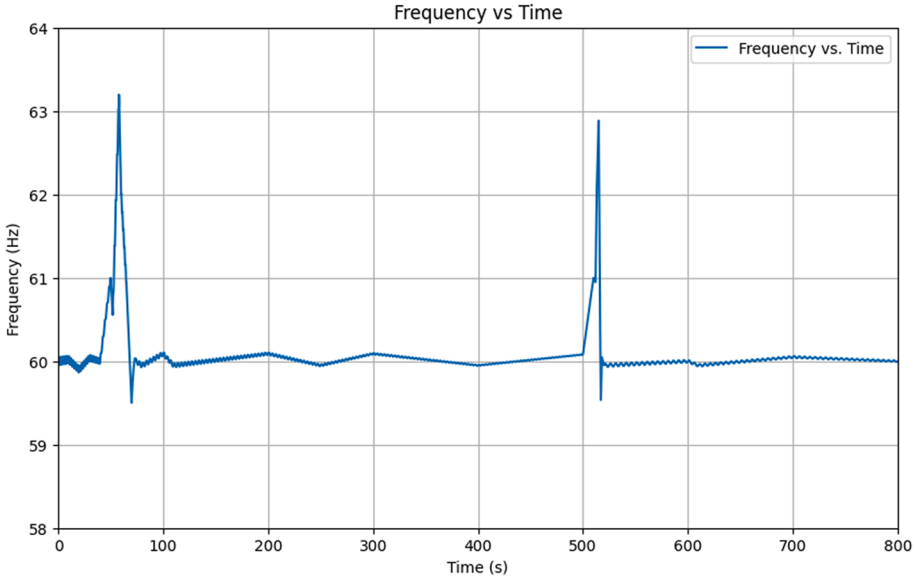


Fig. 9. Recorded frequency oscillations due to the DDoS attacks.

operational baseline for the wind turbine generator, irrelevant of external disruptions. The onset of the first DDoS attack at t = 55 s triggers an immediate and noticeable reduction in power generation. In the absence of control or defensive mechanisms, the cyberattack directly impacts the generator's command and control systems, severing communication with grid operational controls. Consequently, there is a sharp decrease in output, falling significantly below the nominal level, reflecting the generator's incapacity to sustain power production amid the communication breakdown induced by the DDoS attack.

In the period subsequent to the first cyberattack, the generator's output fails to return to its original nominal levels. Instead, it exhibits increased variability, which is uncharacteristic for wind turbine operations under stable conditions. This enhanced variability points to lingering effects from the cyber intrusion, possibly because the control systems remain disrupted without the support of cyber defense mechanisms to aid recovery.

The second DDoS attack intensifies the destabilizing impacts of the initial assault. This subsequent intrusion further disrupts the generator's operational stability, with power output dropping to lower levels than those observed during the initial attack. The oscillatory behavior during the attack's duration suggests ongoing struggles within the generator's control systems to adjust to the erratic signals, or lack thereof, resulting from the cyber disruption. Following the second attack, while the generation output shows signs of recovery, it does not regain the stability observed before the attacks, continuing to exhibit significant fluctuations around a below-nominal average. This persistent instability underscores the generator's compromised operational state in the absence of preventive measures, highlighting the crucial role of such systems in not only maintaining continuous operation of renewable generation assets but also their integration within the broader power grid infrastructure. This emphasizes the need for robust, real-time cyber defense mechanisms capable of detecting, mitigating, and recovering from cyber-related disruptions. The absence of such systems in this simulation demonstrates the extent to which cyber vulnerabilities can affect renewable generation, with potential repercussions for overall grid reliability and security.

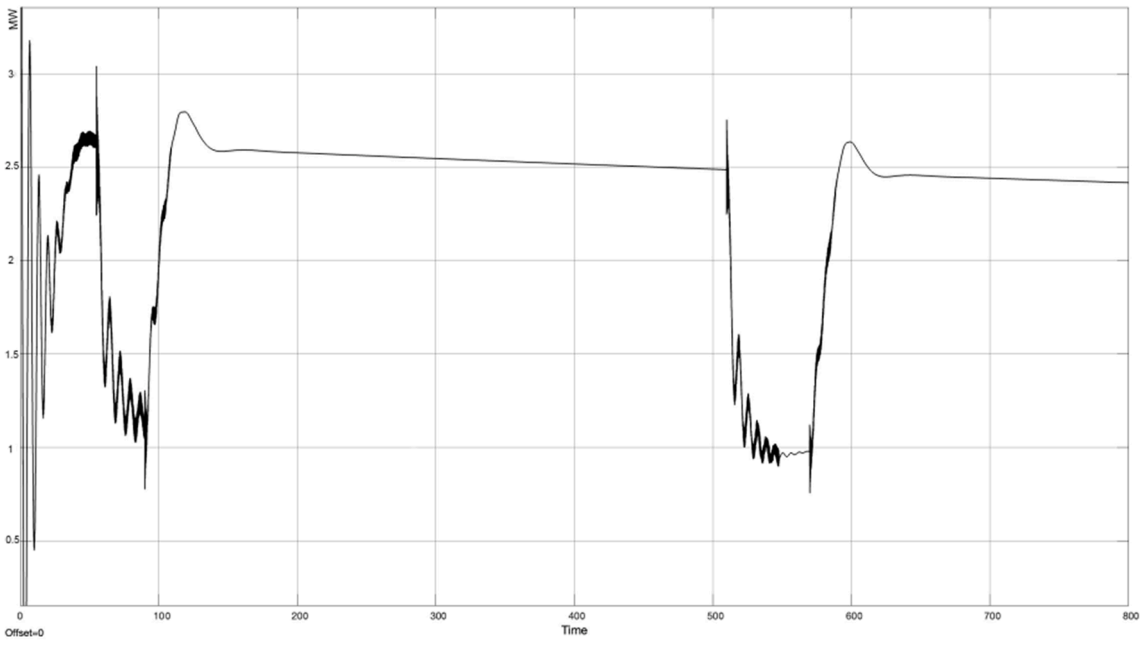


Fig. 10. Oscillation of the wind turbine generator at bus 3 due to the attacks at t = 55 and 510 s.

The effects of the cyberattacks on the three-phase current measurement are depicted in Fig. 11. Prior to the onset of the initial attack, the system operates under typical conditions, with the current magnitude showing minor fluctuations around a nominal value due to transient dynamics in the simulation. The first DDoS attack on the communication link prompts a marked deviation from the nominal current magnitude, characterized by a sharp decrease owing to the cessation of charging activities and resultant reduction in load. Following the identification and resolution of this attack, the current magnitude returns to a more stable state, though with increased variance, reflecting the system's adaptive recovery to the aftermath of the cyberattack. The subsequent attack triggers a more severe disturbance in current magnitude, marked by a sharp decline followed by a volatile recovery phase, suggesting an exacerbated impact due to the sequential nature of the attacks. Post-second-attack recovery shows a reversion to nearly nominal current levels, yet with persistent minor fluctuations, indicating a resilient system contending with sequential cyberattacks. The dual-attack scenario underscores the network's susceptibility to rapid, consecutive cyber intrusions, where the first attack's effects seem to sensitize the system, leading to an amplified response to the subsequent attack. While the system's capacity to restore operational current magnitudes post-attacks evidence robust automated recovery mechanisms, it also underscores the need for enhanced defensive strategies to reduce the variance in current magnitude and bolster overall system stability.

It is imperative to acknowledge that, in practical grid environments, not every EV will be operating at its maximum charging capacity concurrently. Numerous variables, such as the battery's current state of charge, the diurnal cycle, and power regulation strategies implemented by the charging infrastructure or the grid management entity, play a pivotal role in influencing the real-time power consumption.

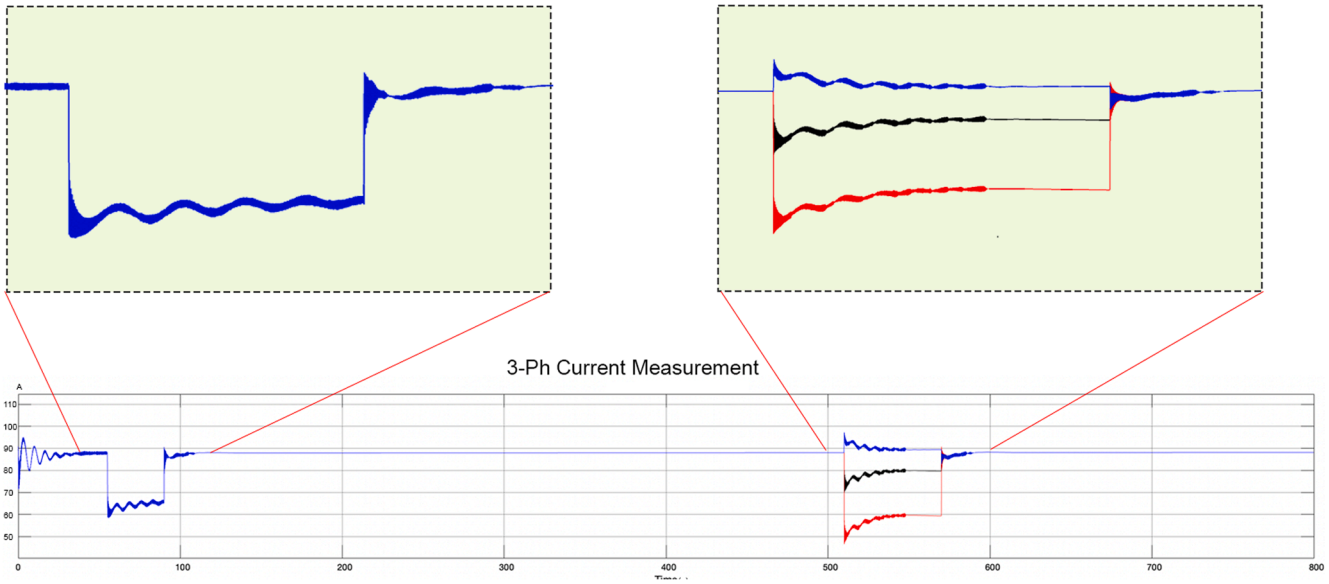


Fig. 11. Variations of the 3-ph current measurement vs time due to the DDoS attacks.

5. Conclusion

In the rapidly evolving landscape of transportation electrification, ensuring the cybersecurity of energy infrastructures will be a central theme in a digitalized world. This work has elucidated the potential utilization of EVs as attack surface vectors for cyberthreats, given their bi-directional communication capabilities within the smart grid ecosystem. This research is motivated by a notable gap in the existing literature, particularly the lack of focused research and public awareness concerning the cybersecurity challenges associated with EVs. The empirical studies conducted on the modified IEEE 33-bus system demonstrate the practical implications of cyberthreats on power distribution networks. The dynamic nature of each bot's attack rate over time, modeled through a combination of foundational and time-variant rates, illustrates the aggregate impact of a DDoS attack on EVCS infrastructure. This complexity is further captured in a transition matrix that details the potential state changes of active bots, essential for accurately modeling the intensity of attacks.

Employing the Ornstein-Uhlenbeck process, this work provides a nuanced understanding of the stochastic behaviors of these cyber-attacks. By integrating queueing theory, specifically the M/G/1 queue model, the study offers insights into the transient dynamics of request arrivals and processing times during an attack. The observed disruptions in both active and reactive power demands at the EVCS, resulting from the DDoS attacks, lead to notable deviations in voltage and frequency within the broader grid network.

Crucially, the successful execution of DDoS attacks reveals significant departures from nominal power settings, directly compromising the stability of the grid. Voltage fluctuations and subsequent frequency anomalies during and after attacks underscore the profound impact of such cyber incidents. In conclusion, as the integration of electric mobility advances, its cyber-resilience becomes indispensable. The resilience of power distribution networks against cyberthreats is crucial for maintaining operational integrity. The findings from this study, particularly the simulation of sequential DDoS attacks, underscore the necessity for advanced, adaptive protection systems capable of mitigating complex cyberthreats and facilitating swift recovery to normal operations.

Building on the insights gained, future research will explore a broader spectrum of strategies to enhance cybersecurity measures within the EVCS environment. This will include the development of comprehensive frameworks that incorporate real-time monitoring, threat detection, anomaly analysis, and automated response mechanisms. In particular, the application of metaheuristic and advanced optimization techniques will play a critical role in refining these strategies. These methods can optimize the configuration and operation of defense mechanisms, ensuring that protective measures are both effective and efficient. By deploying such algorithms, it will be possible to dynamically adapt network configuration, enhance the detection capabilities of IDS, and optimize the allocation of network resources to mitigate the impact of cyber threats. This proactive approach not only enhances the resilience of individual EVCS but also safeguards the stability and reliability of the broader smart grid infrastructure.

CRediT authorship contribution statement

Tawfiq Aljohani: Conceptualization, Formal analysis, Funding acquisition, Methodology, Supervision, Validation, Writing – original draft, Writing – review & editing. **Abdulaziz Almutairi:** Conceptualization, Data curation, Formal analysis, Methodology, Project administration, Visualization, Writing – review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Tawfiq M. Aljohani reports article publishing charges was provided by Kingdom of Saudi Arabia Ministry of Education. No conflict of interest of any kind. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number 445-9-873.

References

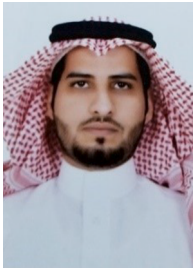
[1] Gungor VC, Lambert FC. A survey on communication networks for electric system automation. Comput Netw 2006;50(7):877–97.
[2] Metke AR, Ekl RL. Smart grid security technology. In 2010 Innovative Smart Grid Technologies (ISGT). IEEE; 2010, January. p. 1–7.
[3] Aljohani TM. Cyberattacks on energy infrastructures as modern war weapons —Part I: analysis and motives. IEEE Technology and Society Magazine. IEEE Technol Soc Mag 2024;43(2). https://doi.org/10.1109/MTS.2024. 3395688.
[4] Aljohani TM. Cyberattacks on energy infrastructures as modern war weapons —Part II: gaps, standardization, and mitigation measures. IEEE Technol Soc Mag 2024;43(2). https://doi.org/10.1109/MTS.2024.3395697.
[5] Wang Y, Zhao Z, Qi B, Cheng Y, Tang K, Li B. Vulnerability analysis of an electric vehicle fleet for car-sharing service under cyber attacks. Sustain Energy Grids Netw 2024;37:101207.
[6] Aljohani T, Mohamed MA, Mohammed O. Tri-level hierarchical coordinated control of large-scale EVs charging based on multi-layer optimization framework. Electr Pow Syst Res 2024;226:109923.
[7] Warraich ZS, Morsi WG. Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids. Sustain Energy Grids Netw 2023;34:101027.
[8] Hasan MK, Habib AA, Islam S, Safie N, Abdullah SNHS, Pandey B. DDoS: distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. Energy Rep 2023;9:1318–26.
[9] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput Commun Rev 2004;34(2):39–53.
[10] Huseinović A, Mrdović S, Bicakci K, Uludag S. A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access 2020;8:177447–70.
[11] Bawany NZ, Shamsi JA. SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks. J Netw Comput Appl 2019; 145:102381.
[12] Chaudhary S, Mishra PK. DDoS attacks in Industrial IoT: a survey. Comput Netw 2023;110015.
[13] Agnew D, Boamah S, Mathieu R, Cooper A, McNair J, Bretas A. Distributed software-defined network architecture for smart grid resilience to denial-of-service attacks. In: 2023 IEEE Power & Energy Society General Meeting (PESGM); 2023, July. p. 1–5.
[14] Pelechrinis K, Iliofotou M, Krishnamurthy SV. Denial of service attacks in wireless networks: the case of jammers. IEEE Commun Surv Tutorials 2010;13(2):245–57.
[15] Temple WG, Chen B, Tippenhauer NO. Delay makes a difference: smart grid resilience under remote meter disconnect attack. In: 2013 IEEE international conference on smart grid communications (SmartGridComm); 2013, October. p. 462–7.
[16] Alnifie G, Simon R. A multi-channel defense against jamming attacks in wireless sensor networks. In: Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks; 2007, October. p. 95–104.
[17] Chai B, Yang Z. Impacts of unreliable communication and modified regret matching based anti-jamming approach in smart microgrid. Ad Hoc Netw 2014;22: 69–82.
[18] Chatfield B, Haddad RJ, Chen L. Low-computational complexity intrusion detection system for jamming attacks in smart grids. In 2018 international conference on computing, networking and communications (ICNC); 2018, March. p. 367–71.
[19] Li H, Lai L, Qiu RC. A denial-of-service jamming game for remote state monitoring in smart grid. In: Proceedings of the 2011 45th annual conference on information sciences and systems, Baltimore, MD, USA, 23–25 March; 2011. p. 1–6.
[20] Shah SQA, Khan FZ, Ahmad M. Mitigating TCP SYN flooding based EDOS attack in cloud computing environment using binomial distribution in SDN. Comput Commun 2022;182:198–211.
[21] Asri S, Pranggono B. Impact of distributed denial-of-service attack on advanced metering infrastructure. Wirel Pers Commun 2015;83:2211–23.
[22] Almorabea OM, Khanzada TJS, Aslam MA, Hendi FA, Almorabea AM. IoT network-based intrusion detection framework: a solution to process ping floods originating from embedded devices. IEEE Access 2023;11:119118–45.
[23] Gupta N, Jain A, Saini P, Gupta V. DDoS attack algorithm using ICMP flood. In: 2016 3rd international conference on computing for sustainable global development (INDIACom); 2016, March. p. 4082–4.
[24] Manso P, Moura J, Serrão C. SDN-based intrusion detection system for early detection and mitigation of DDoS attacks. Information 2019;10(3):106.

[25] Kumar R, Kumar P, Tripathi R, Gupta GP, Garg S, Hassan MM. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. J Parallel Distrib Comput 2022;164:55–68.
[26] Rahman MA, Asyhari AT, Leong LS, Satrya GB, Tao MH, Zolkipli MF. Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustain Cities Soc 2020;61:102324.
[27] Al Ridhawi I, Otoum S, Aloqaily M, Jararweh Y, Baker T. Providing secure and reliable communication for next generation networks in smart cities. Sustain Cities Soc 2020;56:102080.
[28] Zadsar M, Ghafouri M, Ameli A, Moussa B. Time-synchronization attack on data aggregation in wide-area damping controllers. In: 2022 IEEE electrical power and energy conference (EPEC); 2022, December, p. 368–73.
[29] Ghafouri M, Kabir E, Moussa B, Assi C. Coordinated charging and discharging of electric vehicles: a new class of switching attacks. ACM Trans Cyber-Phys Syst (TCPS) 2022;6(3):1–26.
[30] Gaderer G, Treytl A, Sauter T. Security aspects for IEEE 1588 based clock synchronization protocols. In Proc. IEEE Int. Workshop Factory Commun. Syst. (WFCS); 2006, June. p. 247–50.
[31] Fan Y, Zhang Z, Trinkle M, Dimitrovski AD, Song JB, Li H. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids. IEEE Trans Smart Grid 2014;6(6):2659–68.
[32] Xue A, Xu F, Chow JH, Leng S, Kong H, Xu J, et al. Data-driven detection for GPS spoofing attack using phasor measurements in smart grid. Int J Electr Power Energy Syst 2021;129:106883.
[33] Baumgartner B, Riesch C, Schenk W. The impact of gps vulnerabilities on the electric power grid. In: XX IMEKO World Symposium; 2014, September. p. 183–8.
[34] Ismail S, Hassen HR, Just M, Zantout H. A review of amplification-based distributed denial of service attacks and their mitigation. Comput Secur 2021;109:102380.
[35] Zhang Y, Cheng Y. An amplification DDoS attack defence mechanism using reinforcement learning. In: 2019 IEEE SmartWorld, ubiquitous intelligence & computing, advanced & trusted computing, scalable computing & communications, cloud & big data computing, internet of people and smart city innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI); 2019, August. p. 634–9.
[36] Anagnostopoulos M, Kambourakis G, Kopanos P, Louloudakis G, Gritzalis S. DNS amplification attack revisited. Comput Secur 2013;39:475–85.
[37] Gondim JJ, de Oliveira Albuquerque R, Orozco ALS. Mirror saturation in amplified reflection Distributed Denial of Service: a case of study using SNMP, SSDP, NTP and DNS protocols. Futur Gener Comput Syst 2020;108:68–81.
[38] Yang Y, McLaughlin K, Sezer S, Littler T, Pranggono B, Brogan P, Wang HF. Intrusion detection system for network security in synchrophasor systems; 2013.
[39] Huang Q, Kobayashi H, Liu B. Modeling of distributed denial of service attacks in wireless networks. In: 2003 IEEE pacific rim conference on communications computers and signal processing (PACRIM 2003) (Cat. No. 03CH37490), vol. 1; 2003, August. p. 41–4.
[40] Yu S, Tian Y, Guo S, Wu DO. Can we beat DDoS attacks in clouds? IEEE Trans Parallel Distrib Syst 2013;25(9):2245–54.
[41] Aljohani TM, Ebrahim AF, Mohammed OA. Dynamic real-time pricing mechanism for electric vehicles charging considering optimal microgrids energy management system. IEEE Trans Ind Appl 2021;57(5):5372–81.
[42] Knezović K, Soroudi A, Keane A, Marinelli M. Robust multi-objective PQ scheduling for electric vehicles in flexible unbalanced distribution grids. IET Gener Transm Distrib 2017;11(16):4031–40.

Glossary

EVCS: Electric Vehicle Charging Station
DDoS: Distributed Denial of Service Attacks
ICMP: Internet Control Message Protocol
UDP: User Datagram Protocol
TCP: Transmission Control Protocol
TCP/IP: Transmission Control Protocol/Internet Protocol
IDS: Intrusion Detection Systems
PTP: Precision Time Protocol
DNS: Domain Name System
NTP: Network Time Protocol
SNMP: Simple Network Management Protocol
$\lambda(t)$: Time-varying Poisson process
$\lambda(s)$: Rate of bots generated attacks
N: Number of acting bots
Qij: Transition matrix.
$-\lambda_i(t)$: Transitioning rates of the bots.
$P_{ij}(t)$: Probability of changing the state from i to j
$\Lambda(t)$: Cumulative intensity function
$dW(t)$: Wiener process
α, σ: Mean-reversion rate; Volatility rate
$Q(t)$: The queue length at EVCS
$\mu(t)$: Service rate at EVCS
$\beta(t)$: Beta distribution
$\mu_r(t)$: Refreshment to recovery transition rate
$\mu_f(t)$: Refreshment to failure transition rate
$P_{nominal}$: Nominal active power at EVCS
$\Delta P_{attack}(t)$: Change in active power due to DDoS
$Q_{nominal}$: Nominal reactive power at EVCS
$\Delta Q_{attack}(t)$: Change in reactive power due to DDoS
$V_{nominal}$: Nominal voltage level at EVCS
$\Delta V_{ch}(t)$: Deviation in charging voltage levels
$\Delta f_{grid}(t)$: Deviation in frequency levels
M, D: The grid's inertia constant and damping factor

Tawfiq M. Aljohani received his B.S. in Electrical Engineering from King Abdulaziz University (2009), M.Sc. degree in Electrical Engineering (2014), M.Sc. degree in Green Technologies & Sustainability (2017) and a Graduate Certificate in System Architecting & Engineering (2017) all from the University of Southern California. He earned his Ph.D. in Electrical and Computer Engineering from the energy system research laboratories of Florida International University (2021). Dr. Aljohani published in top-tier outlets including IEEE transactions, Elsevier's, and other Q1 outlets and top-tier conferences. His research centers on mathematical modeling of energy dynamics, cybersecurity of energy infrastructure, power system optimization and control, and energy network modernization.



Abdulaziz Almutairi received the B.Sc. degree in electrical engineering from Qassim University, Buraydah, Saudi Arabia, in 2009, and the M.A.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2014 and 2018, respectively. He is an Associate Professor in the Department of Electrical Engineering at Majmaah University, where he also serves as the Director of the Innovation and Entrepreneurship Center. He specializes in electric vehicles, renewable energy and data analysis, and has published several research papers in high-impact journals. Dr. Almutairi is distinguished for his extensive knowledge in the field of electrical engineering, his contributions to research have been widely recognized and he is one of the foremost experts in electric vehicle charging infrastructure in the Kingdom of Saudi Arabia. Dr. Almutairi's commitment is not limited to his academic work, but he is also committed to contributing to society, as he participated in many activities related to social investment, volunteer work, human resource development, and sustainable development projects.