Hidden Markov Models-Based Anomaly Correlations for the Cyber-Physical Security of EV Charging Stations

Mansi Girdhar, *Student Member, IEEE*, Junho Hong, *Member, IEEE*, Hyojong Lee, *Member, IEEE*, and Tai-Jin Song, *Member, IEEE*

***Abstract*—Over recent years, we have seen a significant rise in electric mobility to overcome the anthropogenic emissions by conventional gasoline vehicles. However, the prerequisite of smoothening of peaks and imbalances through bidirectional charging is concatenated with the undesired impacts on reliability and security of power system operation when there are probable intrusions in the eXtreme Fast Charging (XFC) station, hence destabilizing the charging networks. So this paper applies STRIDE based threat modeling to analyze and identify multiple potential threats endured by the cyber-physical system (CPS) of XFC station by using weighted attack defense tree. Potential mitigation strategies are then suggested for the identified severe threats. In addition, this paper also develops a stochastic probabilistic tool, the Hidden Markov Model (HMM) for modeling the security attacks for a given range of identified attack vectors and hence employing an appropriate defense strategy against the malicious hacker. Also, a weighted attack defense tree has been developed to generate various attack scenarios. In the end, the results of the proposed work are substantiated and validated if it is able to considerably improve overall charging efficiency and cyber-physical security of the charging station network.**

***Index Terms*—Electric vehicle charging station, cyber-physical security, hidden Markov models, cybersecurity of EV charger.**

I. Introduction

THE AUTOMOBILE industry begins to transition away from conventional fossil fuel-powered or internal combustion engine-based vehicles (ICEV) to electric vehicles (EVs) for better carbon emission benefits. Since more than 18 million EVs are expected by 2030, it is crucial to have a proper plan of deployment of EV charging stations and robust supporting electric distribution infrastructures for a quick and seamless recharge in order to accommodate the continuously growing fleet of EVs [1]. Moreover, the EV charging stations have been steadily expanding their charging power, e.g., ultra-fast DC chargers [2] or XFC stations with multiple modules. The rated charging power of up to 350 kW can offer faster charging rates within approximately 10 minutes, which is commensurable to the refueling experience of gasoline vehicles [3]. Due to the increased numbers of EVs and demand for XFC stations, the penetration of XFC stations in the electric grids will be increased. It is well known that transmission of large amounts of energy within short time windows can potentially cause electric network voltage instability problems. An attack to take control of and charge all XFCs and local battery energy storage systems (BESSs) at the same time could compromise the operational security and voltage stability of the electric distribution power grid, pushing the whole grid towards instability [3].

Although there is some dedicated research done on the cybersecurity of power grids in the literature, the cybersecurity aspects of the XFC stations have not been fully addressed. Cyber attacks on critical infrastructure systems are evolving, and their patterns are diversifying, particularly for energy delivery systems. An external entity can damage a physical system by compromising its information and communications technology (ICT) infrastructure and gaining more defined access to the supervisory control and data acquisition (SCADA) system to control and monitor the elements of the power grid, either through corporate network, virtual private network (VPN) links, or remote site communication, without requiring a physical attack [4]. In fact, a coordinated cyber attack on the Ukrainian power grid clearly showed the need for reliable cyber-physical security measures at substations and SCADA systems. The first cyber attack was on Dec. 23, 2015 and the second attack on Dec. 17, 2016 [5], [6]. Both attacks successfully compromised the utility's industrial control system (ICS). Thus, malicious cyber intrusions potentially impact the critical infrastructure and can cause equipment failure and cascading power disruptions. It is, therefore, crucial to enhance the cybersecurity of industrial automation and control systems and analyze CPS security holistically to enhance the resiliency and reliability of power systems.

Many research efforts are being carried out in detecting and mitigating these cybersecurity threats in a power grid. These striving efforts have resulted in the development of many cybersecurity standards as well as protocols and also produced several ICT-based defense mechanisms. For

Manuscript received 13 April 2021; revised 10 August 2021 and 10 October 2021; accepted 13 October 2021. Date of publication 21 October 2021; date of current version 23 August 2022. This work was supported by Chungbuk National University Brain Korea (BK) 21 FOUR (2021). Paper no. TSG-00554-2021. *(Corresponding author: Tai-Jin Song.)*

Mansi Girdhar and Junho Hong are with the Department of Electrical and Computer Engineering, University of Michigan–Dearborn, Dearborn, MI 48128 USA.

Hyojong Lee is with the US Hitachi Energy Research Center, Hitachi Energy, Raleigh, NC 27606 USA.

Tai-Jin Song is with the Department of Urban Engineering, Chungbuk National University, Cheongju 28644, South Korea (e-mail: tj@chungbuk.ac.kr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2021.3122106.

Digital Object Identifier 10.1109/TSG.2021.3122106

instance, the Critical Infrastructure Protection (CIP) 002-009 standard was developed by the North American Electric Reliability Corporation (NERC) to ensure the secure and reliable operation of bulk power systems (BPSs) [7]. Likewise, IEC 62351 standard has been developed by the International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15 for the cybersecurity of the industrial communication protocols [8]. Hong *et al.* in [9] proposed an integrated anomaly detection system (ADS) that detects malicious activities and abnormal behaviors in substation automation systems (SAS) in a power grid. However, this anomaly detection is limited to Generic Object Oriented Substation Events (GOOSE) and sampled value (SV) protocols. Also, an ADS was presented in [10] for the reliable transmission of Manufacturing Message Specification (MMS) protocols. The work embodied in [11] propounded a distributed intrusion detection system (IDS) that can detect both power system faults and cyber intrusions. Yang *et al.* [12] elaborated upon a multi-layered IDS to detect anomalies of IEC 61850 based communication protocols and whitelisting. However, there are several unknown security vulnerabilities in the ICT-based (cyber layer) based detection and mitigation methods. They might generate numerous false positives that may reduce the accuracy of breach detection systems and have huge impacts on cybersecurity. Therefore, the work in [6] proposed a cybersecurity layer for mitigating attacks that can improve the accuracy of detection of cyber intrusions. Although previous research proposed efficient and resilient cybersecurity mitigation frameworks for power system applications, they do not normally support the cybersecurity of the XFC stations.

Due to various interactions and interdependencies between cyber and physical components in the EV charging station, the exchanged data might be subject to various vulnerabilities, e.g., denial of service (DoS) attack, man-in-the-middle (MITM) attack, eavesdropping, spoofing, false data injection (FDI), ransomware, and trojan viruses. These attacks could lead to personal or financial data infringement and hijacking of power, EV or XFC [13]. The problem intensifies at XFC level (i.e., high power EV charger) due to the higher accessibility and a large amount of the power flow to EVs. The attackers may use the existing vulnerabilities of EV charger or station equipment to compromise the system. For instance, EV owner may lose their availability of EV charging process due to the DoS attack or safety issue due to the battery overcharging attacks. Moreover, the attack can perform several other manipulations, e.g., limiting the charging rate, blocking battery charging, draining, or overcharging. A cybersecurity company, Kaspersky Lab revealed that EV charging stations are open to hackers [14]. Although charging stations have not yet come across extensive and distinguished cyber attacks, researchers and white-hat hackers have been interfering with the charging process of the stations to discover potential vulnerabilities primarily to facilitate research and awareness.

An EV charging station acts as an interface or a high-wattage access point between an EV and a power grid. Furthermore, attackers may undesirably exploit the compromised XFC station to jeopardize the supply-demand balance of a grid by remotely controlling the charging behaviors of the stations in a scalable manner. For instance, each EV generates critical information (e.g., location, charging time, and average power consumption per hour) at the charging station, which is highly vulnerable. Attackers can cause a sustained, large spike in demand resulting in cascading disconnection of power supply from the power grid and abnormal operation performance (e.g., load casting/dropping synchronously or frequent and synchronous casting and dropping). Subsequently, the power plants would be forced into restart conditions, causing widespread brownouts or blackouts and grid instability. Hence, it can threaten the security and stable operation of the power systems. Thus, the infected EVs may cause cascading effects, and the attacker can gain access to the XFC station and/or the EVs [15]. It is critical to identify and secure the intruding points which can be exploited by the threat actors to gain access to the XFC infrastructure. Therefore, cyber-physical security concerns of the EV charging ecosystem, along with the possible detection and mitigation measures, need to be addressed to ensure safe, secure, and resilient DC fast charging. To address these critical cybersecurity gaps, the European Network of Cybersecurity proposed security standards for several EV charging architectures [16]. Also, the U.S. DOE, NHTSA and, DOHS outlined several cybersecurity challenges and proposed recommendations to enhance EV cybersecurity.

This paper focuses on XFC station cybersecurity and the detection and mitigation of coordinated cyber attacks. The underlying contributions of this paper are: (1) a comprehensive threat modeling framework based on light-weight STRIDE methodology for an XFC station and associated infrastructure to know the existence of potential cyber hazards within the environment, (2) a cyber vulnerability assessment of the assets based on the model using the weighted attack defense tree to identify the potential ramifications associated with the cyber attacks on the XFC station, (3) development of defense strategies to mitigate the impact of cyber intrusions, and (4) development of a statistical tool, HMM to detect and predict the attack phases in a multi-step attack scenario.

The remainder of the paper is divided as follows: Section II presents an overview of the cyber-physical model of XFC station. Section III reviews the framework of the proposed methodology. Section IV outlines the known vulnerabilities in the EVs and XFC station. It is followed by developing and analyzing a STRIDE threat model and weighted attack defense tree to generate various attack scenarios via the known attack vectors in the EVs and XFC station. Section V describes the proposed intrusion prediction and prevention model. Then Sections VI and VII discuss the implementation of HMM based on anomaly correlation in XFC station along with the case studies defining the potential mitigation strategies. This section also evaluates the performance of the proposed framework and compares it with the state-of-the-art algorithms. Finally, Section VIII concludes the paper along with the limitations and recommendations for the future work.

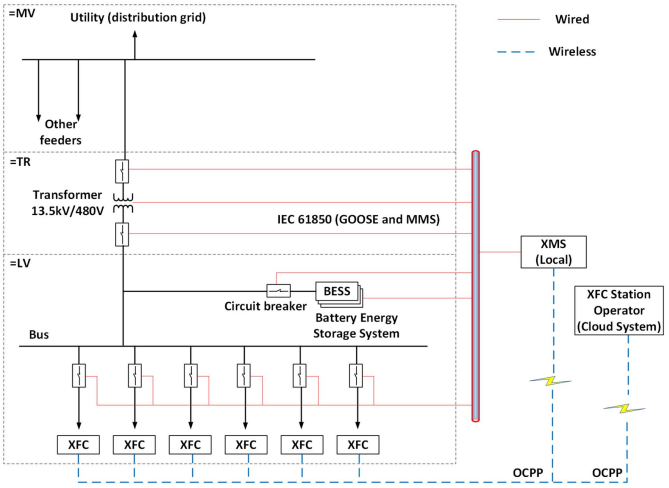

Fig. 1. A cyber-physical system diagram of XFC station.

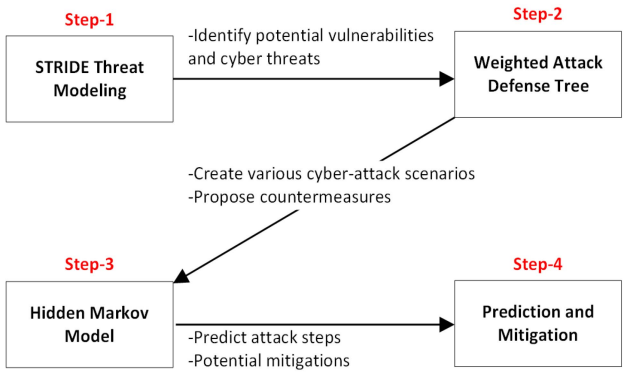

Fig. 2. A pipeline of the proposed framework.

II. Cyber-Physical System of XFC Station

A single-line diagram of a CPS of XFC station is illustrated in Fig. 1. The step-down distribution transformer is connected to the distribution system to provide power to the XFC station [17]. This transformer usually comes with an on-load tap changer (OLTC) to provide maximum reliability. Although this EV charging station is configured with AC internal distribution system for EV chargers, DC bus configuration can be offered for cost-effectiveness solutions [18]. Multiple dedicated XFCs can then be connected through the outgoing feeders in a parallel configuration to recharge the batteries of multiple EVs simultaneously. Also there is a centralized XFC BESS acting as a buffer, integrated into the LV DC link using an AC/DC converter to perform secondary services, such as energy arbitrage, standalone operation in case of grid faults, and other grid ancillary services (e.g., load leveling, power pulsation minimization, and frequency regulation). Therefore, it can provide uninterrupted power to each XFC during periods of congestion on the grid or line losses. It is deployed for power smoothening to reduce the stress on the grid infrastructure. Hence, this structure develops an intelligent system that considers grid congestion [19]. In addition, to enhance the reliability of the distribution network, associated infrastructure components (e.g., switchgears consisting of automatic switches, fuses, reclosers, circuit breakers (CBs), sectionalizers) are installed in the distribution system to control, protect (e.g., clearing faults and interruption of short-circuit) and isolate high-maintenance electrical equipment. The protection equipment (e.g., intelligent electronic devices) and subsystems are connected directly to an Ethernet LAN using optical fibers. The architecture uses the IEC 61850-8-1 GOOSE messaging on the LAN for communications (e.g., breaker trip commands, lockout commands, breaker failure initiation, and reclosing initiation) among protection devices, thereby eliminating hardwired connections. Also, each XFC station is equipped with the central XFC station management system (XMS) that can provide discrete grid services (e.g., peak shaving, voltage control, demand-side management, demand charge reduction, emergency demand response). XMS receives charging requests from EVs/EVSEs and various grid service requests from utility control centers. The XMS is used to provide common access to discrete XFCs from different vendors over Open Charge Point Protocol (OCPP) with the goal of open and interoperable EV charging. XMS consisting of the aggregator server (AS), the monitoring client (MC), and the PC (separated or integrated), can be utilized for the information exchange, e.g., battery status information, and charging information. Moreover, OCPP allows open communication between an Internet-connected charging station and the cloud-based backend where the operators can easily manage accessibility, remotely upgrade firmware, monitor stations, bill users, optimize charging, and other extended functions. EV communication with charging stations is in the form of different message types as defined by the IEC 61850 standard.

III. Framework of the Proposed System

Fig. 2 provides some details about the proposed framework for the study of cyber-physical security framework of EV charging stations. Vulnerability assessments and threat analysis are analyzed at step 1. It can identify the existing vulnerabilities and cyber threats within the EV charging stations. Then diverse attack models are studied at step 2. The weighted attack defense tree is used to create various cyber attack scenarios. Each attack model also proposes potential mitigation actions. The created cyber attack scenarios are collected and used as an input system data for the step 3. HMM has been used to predict the attack steps. Finally, at step 4, the mitigation actions are studied and proposed based on the results of the predictions from step 3. Each component of the framework is described in the following sections.

IV. Vulnerability and Risk Assessment

The EV charging station is usually equipped with a plethora of sensors and actuators, computing units hosting multiple functions, external (BLE, WiFi, LTE, 4G, 5G) connectivity, and poorly configured devices , which will lead to an increasing number of cyber threats and attack vectors. Recent works have shown that cyber attacks on the charging infrastructure are possible and can have severe financial, privacy and safety harms. Threats are often referred to as anti-requirements that allow a malicious agent or attacker to abuse a CPS. Threat

modeling is a technique to identify the security vulnerabilities exploited by the agents in a system, thereby ensuring reliable operations of the system by determining the potential impact and risk associated with exploitation of vulnerabilities and to develop appropriate threat mitigation solutions.

There have been several paradigms for attack, threat and defense analysis that lay the foundation for the work presented herein. One of the widely adopted cybersecurity models, the MITRE's ATT&CK [20], a threat-based model (acronym for Adversarial Tactics, Techniques, and Common Knowledge) is defined as a vulnerability and risk assessment tool used to analyze real-world adversary behaviors based upon their interactions with different entities in a CPS, leading to systematic advancement in cybersecurity defenses. It is a granular model that defines multiple tactics and techniques leveraged by the attackers, from initial access, execution, all the way through command and control and data exfiltration to interrupt critical service delivery by disrupting ICS processes. It is organized as a matrix of different patterns or stages of an attack (often derived from Cyber Kill Chain model), mapping-out progressive tactics and corresponding techniques. The framework underscores the knowledge of adversary tactics, techniques, and procedures (TTP) that are exploited by the attackers (e.g., applications and protocols used by ICS operators, cyber-physical interfaces). This knowledge base is instrumental for cyber defense teams to centralize research and threat intelligence reports based on real-time attacking techniques and subsequently design effective cybersecurity strategies to protect the infrastructure. Though it is more flexible and comprehensive, there are significant overlaps between ATT&CK and Lockheed Martin's Cyber Kill Chain [21] approach. It is also a seven-phase operational model, defining multiple stages of an attack.

A literature review has identified numerous system safety and security modeling methodologies: (1) system theoretic process analysis for security (STPA-sec) that focuses on system safety and security, (2) hazard and operability (HAZOP) that focuses on system hazards and functions, (3) security-aware hazard and risk assessment (SAHARA) that focuses on system hazards, risks and security, (4) process for attack simulation and threat analysis (PASTA) that focuses on process threats and risk mitigation, (5) operationally critical threat, asset, and vulnerability evaluation (OCTAVE) that focuses on operationally critical threats and assets, and (6) STRIDE that focuses on identification and elimination of potential threats at the component level [22]. The STRIDE threat modeling is an efficient approach focused on cybersecurity, while others are highly complex with more focus on safety and risks [23]. This paper is proposing the integration of STRIDE in the CPS design due to several reasons: (1) it is currently the most mature threat modeling approach, (2) it evaluates the detailed system design by building data flow diagrams (DFD) and identifies cyber threats against each system entity, (3) it is comprehensive and analyzes security properties against each system component, and (4) it ensures system security at the component level. Apart from that, this model is widely adopted as a cybersecurity framework to secure the critical infrastructure from cyber attacks in CPS.

A. STRIDE Model for Threat Analysis

STRIDE is a categorical risk assessment model and has been applied in many CPSs in the past [23], [24]. As shown in Fig. 3, this paper adopted STRIDE model to identify the potential vulnerabilities of the XFC station. It shows the high-level overview of the connectivities and potential vulnerabilities between the charging station, EV chargers and EVs. It represents a mnemonic for six different types of security threats as described below.

1) **S**poofing (External Entity): It refers to masquerading of a legitimate source, process or system entity by falsifying data. A threat agent can hijack the XMS and steal highly sensitive data, e.g., credit card information, personal information, charging time, and payment amounts. It can also gain access to EV/EVSE or install a remotely accessible malware virus that modifies the firmware to accept unauthorized remote command sequences. Updating the firmware would allow for the injection of additional functionality to the attacker, such as methods for maintaining communication with the XMS. Further, compromise in any of the authentication interfaces (e.g., Mobileapp, RFID, and NFC) installed at the XFC station can reveal sensitive authentication details (login credentials) of the EVSE and user to the attacker. The attacker can duplicate this information to imitate EV charging. The infected EVSE not only affects individual EVSEs, but also has a probability of propagating to a network of EVSEs. The malware injected in EVSEs can also pass to EVs, XMS, and the power grids resulting in a temporary shutdown of XFC station [25].
2) **T**ampering (Data Store or Process): It refers to an unauthorized alteration of legitimate information [26]. Also called data corruption, this attack is widely identified as FDI attack. For example, the charging port or EVSE might inject wrong charging or discharging data into XMS. FDI aims at manipulating XMS and various data exchanges between EVs, EVSE, and XMS, e.g., energy request, energy usage, price signal from a utility, demand response (DR) bidding from EVSE, DR request from the utility, event messages, EV ID, and premise location ID (utility ID and customer ID). Hence, the results of the successful tampering attacks on the XFC station could mislead the charging (overcharging the batteries) and grid operations that can cause several damages to the EVs, EVSE, XMS, and even to the grid by damaging the distribution transformer.
3) **R**epudiation (External Entity or Process): It means denying or disowning a certain action executed in the system [26]. Since most of the operations at XFC station are exchanged via communication protocols, there is a risk that both sender and receiver will deny their abnormal actions. For instance, an EV owner has paid the charge process fee, but the compromised XFC denies getting the payment. In this case, EV owner will get a financial problem and will be unable to continue the charging process. In the worst case, the compromised XFCs will deny the charging commands

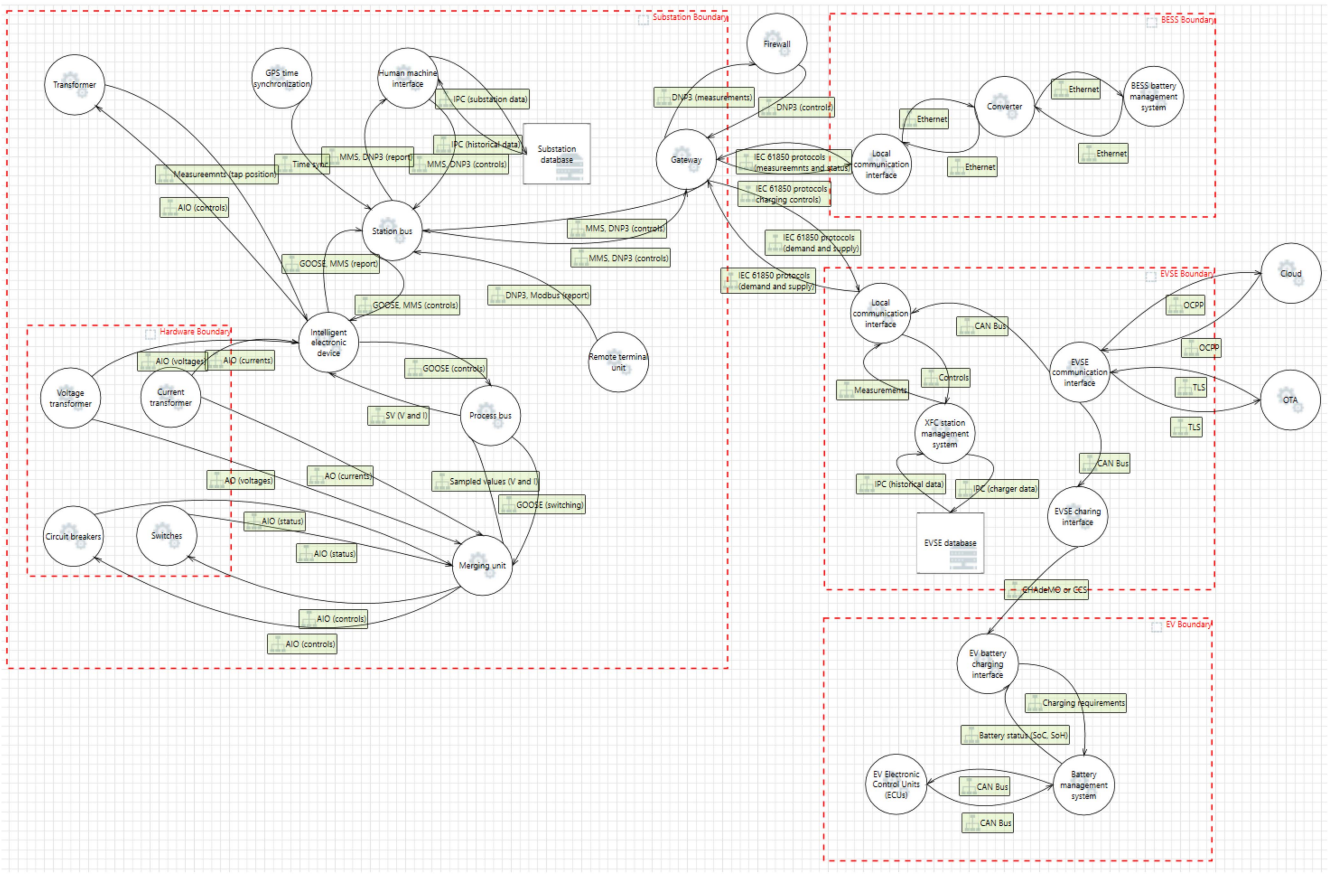

Fig. 3. STRIDE model for threat analysis of the EV charging station.

from the XMS and this will disrupt the overall XFC operations.

4) **I**nformation disclosure: It is denoted as data breach or unauthorized access to security-sensitive information [26]. For instance, the communication between the EVSE and EV over wireless or wired charging connector is highly vulnerable to be intercepted by the threat agent. Hence, the attacker can gain access to the sensitive information (e.g., login credentials, vehicle telematics, and billing information) during the data exchange between XFC vendor and EVs. Both EV and its owner's privacy are at potential risk due to easy interception of EV ID transmitted with the EV charging profile from the EV to EVSE using human machine interface (HMI). The attacker can replicate an invalid EV as an authorized EV and use these details to get free charge. Therefore, it can cause an imminent financial loss to the EV owners as well as the service providers.
5) **D**enial of Service (Data Store or Process): It causes the disruption of timely access of network services to intended users as a result of an attacker's action to jam and overload the bus network by sending a continuous stream of malicious traffic [26]. An ultimate goal of DoS attack is to suddenly shut down the services of an XFC station, i.e., termination of the charging process of connected EVs. In the case of XMS and its entities, attackers can attack servers and deny charging requests from authorized EVs. Due to denial-of-charge (a type of DoS in XMS), important emergency vehicles (e.g., ambulance, fire trucks, and security vehicles) may be denied from charging which will result in detrimental effects on various emergency services and society.
6) **E**levation of privilege (Process): It occurs when a threat actor gets more privileges to access more data in the system as compared to the legitimate user with restricted authority [26]. Primarily, information disclosure or authentication failure may cause this. The entire XFC station could also be compromised due to data poisoning. It includes brute force attack, where the attacker gets access to the EV credentials and exploits the vulnerabilities. For instance, if a malicious attacker gets crucial details of EVSE data (firmware, and user data), they might compromise data and disrupt the XMS functions, create backdoors, add more users, change files or configurations, and other modifications according to their needs.

B. Weighted Attack Defense Tree

A threat modeling is performed for an XFC station using STRIDE model with the weighted attack defense tree. STRIDE model analyzes vulnerabilities against each system component or asset which could be exploited by an attacker to

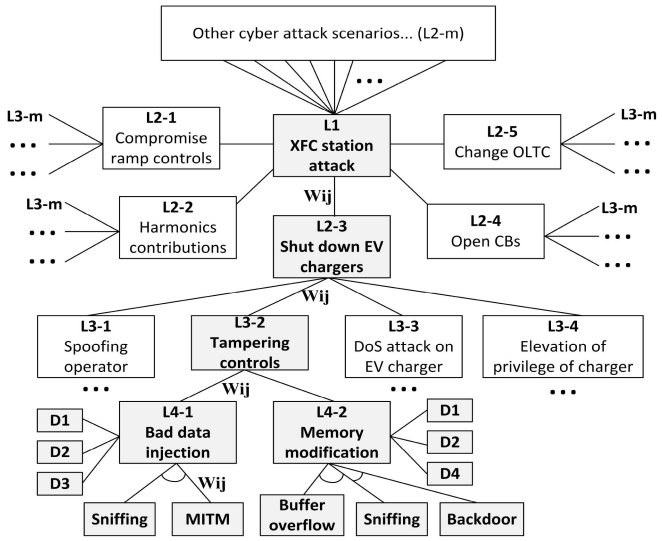

Fig. 4. An example of weighted attack defense tree.

compromise the XFC station. Threats may emerge from different sources, e.g., authorized (internal agents) or unauthorized (external agents) users. Also, they can be generated from a variety of cybersecurity failure scenarios, including problems due to the compromised equipment functionality, data integrity attacks, communication failures, or human errors.

Fig. 4 shows a portion of the proposed weighted attack defense tree for the XFC station. It describes a cybersecurity analysis by identifying adversary's objectives of attack using a graphical, structured tree notation of multiple coupling attack leaves from each node. Besides, it exhibits a multi-level hierarchy in a predecessor-successor structure that states the probable steps taken by the attacker against a system to achieve sub-goals. The root node of an attack tree (e.g., L1: XFC station attack) is the primary goal of an attacker with different combinations of concrete attacks or sub-goals. An attack leaf can be a part of multiple attack scenarios, contingent on its associated node connectivity. Each attack leaf may include one or more defense nodes (to provide countermeasures) acting as successors and logical nodes ("AND" and "OR") acting as predecessors of the attack leaf. For instance, the goal of group L2-3 (i.e., third attack scenario in level two) is to shut down EV chargers by various cyber attack scenarios. One of the scenarios (i.e., L3-2) is tampering with control command signals. The pre-conditions of this attack are: an attacker can control the EV charger via XMS, a user interface of the XFC station operator's system, local/external communication networks. The goal of this attack can be achieved with two different attack scenarios, e.g., bad data injection (L4-1) and memory modification (L3-2). The bad data injection attack has one "AND" condition, i.e., (1) sniffing and MITM. Whereas the memory modification has two "AND" conditions, i.e., (1) buffer overflow and sniffing, and (2) sniffing and backdoor. The post-condition of this attack is that the attackers will tamper the control of the EV chargers, and they can shut down all EV chargers within the XFC station. Mitigation actions have been proposed at each attack scenario (L4-1 and L4-2) for defense strategies. W_{ij} represents a weighting factor (e.g., between each node) that can be used for defense cost (by operator) or attack cost (by attacker). By changing the weighting factors, more various attack scenarios can be generated under different circumstances. Defense cost, which includes hardware equipment, software development, labor, and time costs, is a parameter of paramount importance for developing defensive strategies in a CPS [27]. If the average defense cost for each attack node is \$20,000, the total defense cost will be \$300,000 for the model of 15 attack nodes. This will be a huge investment for any XFC station network operator. So, a minimum defense cost needs to be established by the defender to secure the optimal attack nodes during the design process. In addition, a vulnerability index (V_k) is also a crucial factor [28] to identify the vulnerable components within the XFC station. The vulnerability index can be represented from 0 to 1 (from the most vulnerable (0) to the least vulnerable (1)). It is a quantitative indicator of the challenges faced by the attackers in compromising an attack leaf. Hence, the optimal defensive strategy (ODS) can be illustrated by minimizing W_{ij} and maximizing V_k,

$$\textbf{ODS} = min \sum_{i=1}^{N} \sum_{j=1}^{M} W_{ij} + max \sum V_k. \tag{1}$$

There have been a set of high-risk failure scenarios defined by NESCOR for distributed energy resources (DERs) functional domain, which is responsible for delivering power and ancillary services to the electric grid [29]. Electric transportation (ET) system is one of the elements of DERs. As a result, there are many failure scenarios generated through attack tree methodology on different ET system components, including EV, EVSE, EV management server, CAN bus and other intermediate devices. In order to cover more aspects of the connectivity between power grid and EV charging station, this paper focused on more complexed and fast progressing failure scenarios.

V. Intrusion Prediction and Mitigation System

With the intervention of cloud computing in the critical infrastructure today, cyber attacks are evolving and becoming more and more sophisticated due to enhanced intelligent planning with respect to target systems. This paper shows that attackers could exploit multiple vulnerabilities and execute malicious activities inside the XFC station and its ecosystem, thus compromising the security of the system. Therefore, it is crucial to develop effective algorithms and tools to track and predict attack steps in advance to possibly prevent attacks and minimize the damage.

We use a novel framework as a probabilistic predictive model called HMM to model the interactions between the attacker and the XFC station system for each multi-step attack scenario to predict the subsequent step of the attacker. In general, it is a stochastic or probabilistic modeling approach in which system being modeled is assumed to be a Markov process with unobserved states. The basic architecture used for the proposed HMM as a multi-step attack prediction model in the XFC station is illustrated in Fig. 5.

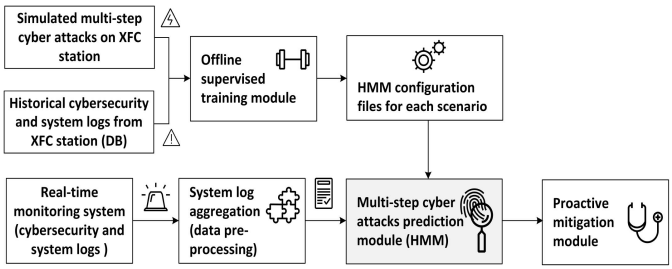

Fig. 5. The flow diagram of the proposed intrusion prediction and mitigation model.

Multi-step attack files that correspond to the correlated attack steps of an attacker to compromise the station (e.g., simulated cyber attacks using the proposed weighted attack defense tree and historical data from the database) are provided as training data for multiple HMMs. The offline supervised training module represents the training phase of the parameters of the proposed HMM-based on observations of different attacks. The HMM configuration files represent the parameters of the HMM after training with different attack scenarios. These files include probability matrices as state transition probability matrix, emission probability matrix, and the number of transition states of the Markov chain. This information is needed in the attack prediction module to evaluate each cyber attack step on the XFC station. The module applies an HMM algorithm to the sequence of alerts arriving from the real-time monitoring system, using an HMM configuration file. The alerts aggregation determines if the alerts and notifications belong to an attack in progress or indicate a new attack. Furthermore, this module could reduce the false positive to negative alerts ratio as low as possible (this function will be implemented in future research). Therefore, the sequence of states the attack goes through or the steps taken by an attacker are assessed. This is then used in a proactive mitigation module to devise appropriate mitigation solutions for the attacks.

VI. Hidden Markov Models

A. Hidden Markov Model Definition

Mathematically, an HMM is defined as two stochastic processes [30]: (1) a hidden process, represented by a random variable $x(t)$ which corresponds to the transitioning between states of the Markov chain, and (2) an observation process, represented by a random variable $y(t)$ and corresponding to the output sequence of observations or emitted symbols from each state, which is used to observe the hidden states.

In the proposed model, several correlated attack steps of the threat agent to compromise an XFC station constitute the hidden stochastic process, and the alert stream generated by the real-time monitoring system correspond to the emitted observations. Here, t represents discrete time, corresponding to the arrival of alerts from the monitoring system.

Hence, a discrete first-order HMM is characterized by

$$\lambda = (\Sigma, S, A, B, \pi) \tag{2}$$

where Σ represents a set of finite observations based on alert sequences such that

$$\mathbf{\Sigma} = \{x_1, x_2, x_3, \ldots, x_M\}. \tag{3}$$

The observations from the monitoring system of a particular multi-step attack are represented by the observation sequence where each component $o(t) \in \mathbf{\Sigma}$,

$$\mathbf{O} = \{o_1, o_2, o_3, \ldots, o_T\}. \tag{4}$$

$\mathbf{S}$ represents a set of finite HMM states based on attack-steps of the attacker such that

$$\mathbf{S} = \{S_1, S_2, S_3, \ldots, S_N\}. \tag{5}$$

$\mathbf{A}$ is an $N \times N$ state transition probability matrix for N possible states, which describes probability of transitioning (a_{ij}) from state i to state j, such that

$$\mathbf{A} = \left\{\{a_{ij}\}_{N\times N} \mid a_{ij} = P\big(q_{t+1} = S_j \mid q_t = S_i\big)\right\}, \quad \text{where } 1 \le i, j \le N \tag{6}$$

$\mathbf{B}$ is an $N \times M$observation or emission probability matrix, which is composed of probability vectors (denoted by b_j) for each state. This vector indicates the observation probability of different alerts for a particular attack scenario,

$$\mathbf{B} = \left\{\{b_j(k)\}_{N\times M} \mid b_j = P\big(x_k \mid q_t = S_j\big)\right\}, \quad \text{where } 1 \le j \le N, 1 \le k \le M. \tag{7}$$

$\mathbf{\Pi}$ is the initial probability distribution vector ($N \times 1$) specifying the probability of the initial state of the attack, i.e., the probability with which the attack can start in each state,

$$\mathbf{\Pi} = \left\{\{\pi_i\}_{N\times 1} \mid \pi_i = P(q_1 = S_i)\right\}, \text{where } 1 \le i \le N. \tag{8}$$

B. Supervised Training Algorithm

There are basically three problems associated with any HMM and in this paper, we are focused on finding the most likely path of states given the model and observation sequence, using the Viterbi algorithm, for which offline training is performed to maximize the probability of the observation sequence for the given model. There are different algorithms for learning HMM parameters from training data, (1) unsupervised training algorithm (Baum-Welch, Expectation Maximisation (EM), Generalised EM (GEM), and the gradient descent method), and (2) supervised training algorithm. In our case, a supervised algorithm is applied (due to its advantages over unsupervised training) to train the HMM by running multiple iterations until the model converges to a critical point [30]. It maximizes the joint probability of the symbol and state sequences. In this training, transition (a_{ij}), emission ($b_j(k)$) probabilities, and initial distribution vector (π) are estimated from samples of multi-step attacks. This is done by counting frequencies of transitions between states and emissions of symbol observations within each state. These frequencies are then normalized into probability estimates. Supervised training is defined by a set of equations:

$$a_{ij} = \frac{a(i,j)}{\sum_{\alpha=0}^{N} \alpha \cdot a(i,\alpha)}, \tag{9}$$

$$b_j(k) = \frac{e(j,o_k)}{\sum_{\alpha=0}^{M} e(j,o_k)}. \tag{10}$$

So, after obtaining both the probability matrices ($\mathbf{A}$ and $\mathbf{B}$) and initial distribution vector ($\mathbf{\Pi}$), the Viterbi algorithm (used

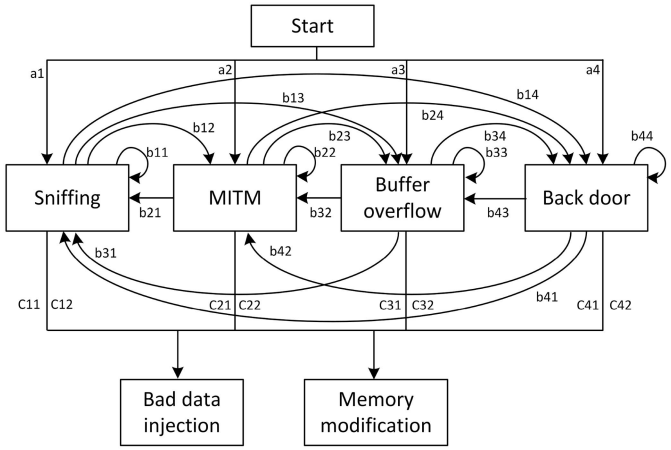

Fig. 6. The states of Markov chain for shut down EV chargers attack.

to compute the best state path for a particular alert observation from real-time monitoring system) is applied to the transition matrix for each HMM configuration to obtain the state sequence. As a result, we can select a specific attack scenario and attack phase represented by transition state chain **S**. This algorithm estimates the best state path or the best state sequence, $\mathbf{Q}* = \{q_1, q_2, \ldots, q_k\}$, for the given alert sequence, $\mathbf{X} = \{x_1, x_2, \ldots, x_k\}$ based on the state probability for each attack step in the Markov chain. This state probability is then used to calculate the final attack probability. The likelihood of best state sequence can be evaluated by the following formula:

$$argmax\{P(X \mid O, \lambda)\} = argmax\{P(X, O \mid \lambda)\}. \tag{11}$$

Let $\delta_t(i)$ be the maximal probability of state sequences at time t that ends in state S_i and produces the first t observations for the given model, denoted by the following formula:

$$\delta_t(j) = max\Big\{P\big(S_1, S_2, \ldots, S_t, x_1, x_2, \ldots, x_t, q_t = S_j \mid \lambda\big)\Big\}. \tag{12}$$

Hence, the Viterbi algorithm computes the best state sequence and specifies the best state S_i at time t.

VII. Case Studies

A. Case Study 1: Tampering XFC Controls

In this section, we will illustrate our approach by a case study of an XFC station network. We construct an attack scenario that involves a sequence of attack stages for shutting down the multiple XFC chargers as an example. The proposed HMM model, as illustrated in Fig. 6, consists of two layers: the hidden states at the first layer and the observable events emitted from the hidden states at the second layer.

The state-space used in the model consists of the following attack states in the first layer.

1) Sniffing (attack state `S`): It indicates that the attacker is at a passive stage and trying to intercept the sensitive data (e.g., passwords and usernames) being exchanged between the EV and EVSE. In this state, the attacker gains access to the network path but is unable to modify the data.
2) MITM (attack state `M`): It indicates that the attacker is at an active stage and attempting to bypass a secured system by impersonating both the EV and EVSE. Hence, it intercepts all the transmissions between the victims and then manipulates the transmitted data.
3) Buffer overflow (attack state `BO`): It indicates that the remote attacker is trying to input malicious data into the memory or buffer, hence corrupting or overwriting fragments of the memory space. It can lead to a station crash as the attacker can change the behavior of the charging application by executing malicious actions. For example, attackers can exploit this attack to control the charging process by connecting to the target's WiFi network, causing physical damage to EV or fire.
4) Backdoor (attack state `BD`): It indicates that the attacker has high-level user access to the XFC station and its network and now can steal data, hijack XMS, install additional malware and control the charging/billing operations and can even shut down the XFC station.

The real-time monitoring system employed in the system monitors the threat agent's user and file access activities and generates alerts and charge interruptions in order to detect the malicious events or abnormal user activities in the station network. It is followed by filtering of trivial alerts and identification of false positive alerts. In our work, we will use two alert sequences as observations which form the second layer, (1) bad data injection (BI) and, (2) memory modification (MM). In a real working environment, more alerts could be used, but for illustrative purposes we limit the number of alert sequences to get smaller matrices for the sake of simplicity. In this paper, we have used historical alert data to build the HMMs for different attack scenarios by employing an offline supervised training algorithm to obtain the trained probability matrices and initial distribution vector given below.

(1) The state transition probability matrix is defined as

$$\mathbf{A} = \begin{Bmatrix} 0.712 & 0.081 & 0.097 & 0.110 \\ 0.008 & 0.809 & 0.105 & 0.078 \\ 0.071 & 0.098 & 0.805 & 0.026 \\ 0.087 & 0.072 & 0.009 & 0.832 \end{Bmatrix}. \tag{13}$$

(2) The emission probability matrix is defined as

$$\mathbf{B} = \begin{Bmatrix} 0.573 & 0.427 \\ 0.969 & 0.031 \\ 0.017 & 0.983 \\ 0.022 & 0.978 \end{Bmatrix}. \tag{14}$$

(3) The initial probability distribution vector is defined as

$$\mathbf{\Pi} = \begin{Bmatrix} 0.282 & 0.257 & 0.211 & 0.250 \end{Bmatrix}. \tag{15}$$

Afterwards, HMM detects and predicts unknown multiple attack phases of the threat agent by applying the Viterbi algorithm to obtain the most likely path of different attack scenarios when the alerts are triggered from the real-time monitoring system indicating malicious intrusion into the XFC station. According to the proposed attack scenario, the system determines that the most likely attack state transition is "M," "M" and "BO" when alert observations for "BI," "BI" and

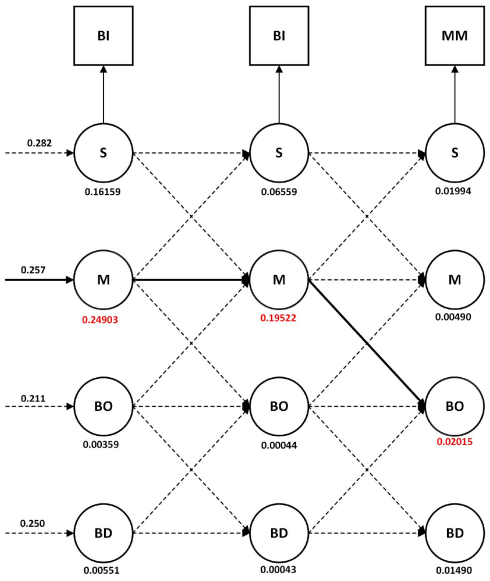

Fig. 7. Viterbi algorithm to detect attack state transition for case study 1.

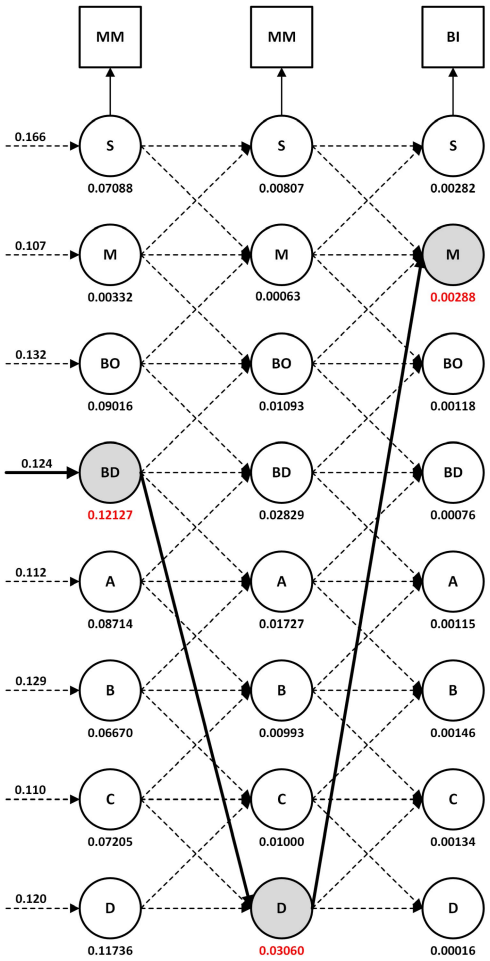

Fig. 8. Viterbi algorithm to detect attack state transition for case study 2.

"MM" are received from the monitoring system at three consecutive times. As demonstrated by the Fig. 7, the most likely attack state (at $t = 1$) is "M" with a maximum probability of 24.9% for the BI alert, the most likely attack state (at $t = 2$) is "M" with a maximum probability of 19.5% for the BI alert, and the most likely attack state (at $t = 3$) is "BO" with a maximum probability of 2.02% for the MM alert. In other words, the threat agent tries to intrude into the XFC station by attempting a series of MITM attacks and buffer overflow attack. Since the networks are highly swamped by the alerts nowadays, so we can use ample alerts to identify the attacks extensively.

B. Case Study 2: DoS Attack

In this case study, we will illustrate a sophisticated attack scenario where EV chargers are compromised by the DoS attack. This scenario involves a sequence of attack stages for the DoS attack on the EV chargers. The state-space used in the proposed model consists of the following eight attack states in the hidden layer, (1) malformed packet (attack state M), (2) protocol vulnerability exploitation (attack state P), (3) network flooding attack (attack state NF), (4) amplification attack (attack state A), (5) multiple login attempts (attack state ML), (6) malware installation (attack state MI), (7) file systems modification (attack state FM), and (8) application flooding attack (attack state AF). Furthermore, we have two alert sequences as observations for the second layer, (1) network bandwidth depletion (NB) and, (2) system resource depletion (SR).

According to the proposed attack scenario, the system determines that the most likely attack state transition is "A," "AF" and "P" when alert observations for "SR," "SR" and "NB" are received from the monitoring system at three consecutive times. As shown by the Fig. 8, the most likely attack state (at $t = 1$) is "A" with a maximum probability of 12.13% for the SR alert, the most likely attack state (at $t = 2$) is "AF" with a maximum probability of 3.06% for the SR alert, and the most likely attack state (at $t = 3$) is "P" with a maximum probability of 0.29% for the NB alert. In other words, the threat agent tries to invade the XFC chargers by attempting a series of SR attacks and NB attack.

Please note that the proposed HMM and Viterbi algorithm are evaluated as an online decoding process to prove the theoretical approaches. It explicates the hidden layer's topology, applicability and then subsequently evaluates the performance of the algorithm. Despite its prohibitive time and space complexity, it has a capability of adding redundant information to correct the wrong information transmitted (called as forward error correction) and reconstruct the lost data. Also, the state or trellis diagram provides a comprehensive description of the system. However, real-time implementation and operation need to be evaluated for future research.

Hence, the proposed model is successfully able to anticipate the cyber intrusions into the XFC station as it renders explicit information on the current state of the attack. Further, the gained knowledge of attacks can be exploited to develop significant mitigation measures to reduce the likelihood of severe impairment caused to the XFC station and grid equipment. In addition, decision of proactive response becomes easier and less complicated.

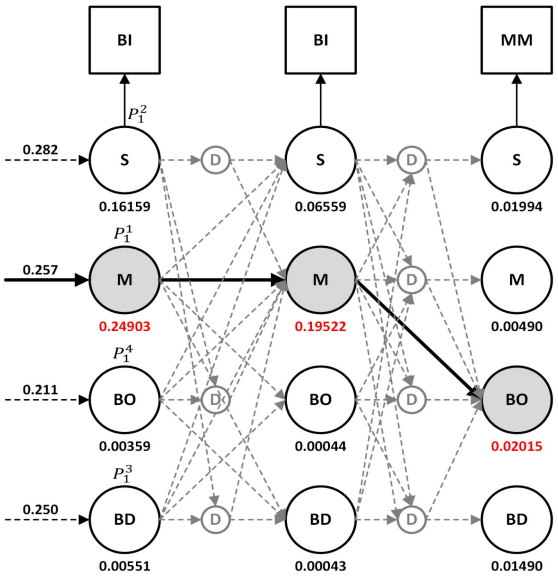

Fig. 9. Deployment of decoy nodes with the predicted path in the station network.

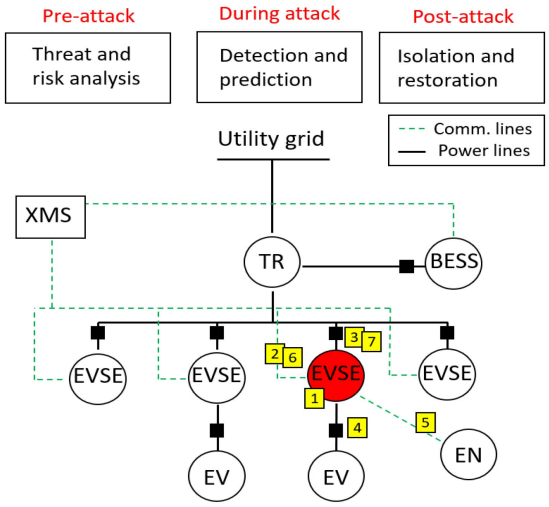

Fig. 10. An example of the mitigation framework.

C. Partially Observable Monte-Carlo Planning (POMCP) Algorithm

A highly skilled and well-trained attacker might not follow the most likely path and cause abnormal behaviors by intruding through alternative attack paths. Hence, to mitigate the other attack paths or vectors, defenders may further employ a POMCP algorithm to guide the attacker towards the predicted path whenever the attacker drifts away from the predicted path [31]. Furthermore, the un-predicted attackers' behaviors could be prevented by deploying decoy nodes along with the predicted paths in the network to deceive the attacker. Then the defenders will receive alerts caused by malicious intrusions if an attacker breaks into the decoy system, and it will be directed towards the predicted paths, as shown in Fig. 9. Therefore, the attacker could be inhibited from compromising the real goal state. It might help the defender undertake several mitigation measures or defense actions to block the attacker beforehand and further avert its malicious actions. In this case, the proposed HMM can cover all potential attack scenarios, and the defenders can focus on the multiple attack scenarios based on the predicted probability index (P_L^{Pr}), where P is probability estimate of an attack state, Pr is priority given to the attack stage, and L is ith layer (i = 1, 2, 3). As illustrated in Fig. 9, an attacker may traverse through any attack path to reach its final goal. Assuming that there is an attack at the "S" attack stage, $P_1^1 = 0.24903$ (the highest probability index at the first layer). Then the presence of decoy nodes (represented as D) along with the predicted path nodes (discovered by the application of HMM) in the network traces the attacker back to the path (i.e., S-M-BO). Even though the implemented decoy has been compromised by attackers, the next predicted path nodes will guide the attackers to another decoy in the system. Hence, the defenders could protect the network against the impending damage from intrusion by deploying active mitigations across each nodal path.

D. Potential Mitigation Strategies

Like any other connected devices, charging stations are vulnerable to a plethora of cyber threats without proper cybersecurity measures. Potential targets may include hardware and software platforms, e.g., XMS, cloud system, BESS, or communication links. A threat agent could remotely identify and exploit numerous cybersecurity breaches and vulnerabilities to launch a DoS, tampering or load alteration attack, and can revoke the charging process. Moreover, the attack can perform several other manipulations, e.g., limiting the charging rate, blocking battery charging, draining, or overcharging. Attackers can potentially use the existing vulnerabilities to install malware or copy highly sensitive information or unlock the charging station devices by manipulating the socket locking hatch. Therefore, it is crucial to design appropriate defense and mitigation strategies to enhance the security and resiliency of the XFC station.

Mitigation refers to the reduction of losses caused due to any undesirable events (cyber attacks) that occurred in a CPS. This paper develops various mitigation strategies to address all three high level phases of cyber intrusion: (1) pre-attack, (2) during attack, and (3) post-attack, as illustrated in Fig. 10. During the pre-attack stage, risk assessment methodologies has been executed to protect different system devices which could be attacked by using different potential avenues. For instance, in this paper, STRIDE is used for threat and vulnerability analysis in the early development cycle. Besides, to meet the minimum cybersecurity requirements, several countermeasures can be used, e.g., vulnerability scan prior and post EV charger installation, multi-authentication, detection of abnormal activities using signature-based cryptography mechanism of EV charger operation and communications, implementing role-based access control (RBAC) approach to restrict access of the XFC station to the authorized users. Similarly, communication paths between the EVs and XFC station can be strongly encrypted and authenticated or anomaly detection systems to detect the abnormal activities between the EV and station can be designed to disconnect the attackers to ensure

secure communication. During the attack phase, the proposed HMM can be used to study the current and future behavior of the attacker, which decides the application of mitigation strategies. For instance, in accordance with the case studies, several mitigations can be employed by predicting the attack states through generating alert sequences. However, for the post-attack mitigations to resume the attacked and damaged EV station to its healthy state, digital forensics can be done by the system engineer (EN), where the compromised equipment (e.g., EVSE) is identified, the source is understood, and compromised data is recovered to maintain a robust security system. Furthermore, system hardening to reduce its vulnerability surface can be done by isolating (by disconnecting the compromised distribution feeder by opening CB, and/or disabling the compromised communication ports by managed communication switches) and substituting the compromised asset with a safer backup system that can be used until the original system resumes to its normal operations. Other protective measures adopted by the EN may include updating the firmware/security updates or removal of unauthorized software, setting up IDS or intrusion prevention system (IPS) to reserve the issue during maintenance or patch account management to achieve cyber restoration. As illustrated in Fig. 10, (i) the proposed active mitigations will evaluate the cyber vulnerabilities of the XFC stations during pre-attack phase, (ii) during the attack phase, ongoing cyber attacks will be detected and predicted by the proposed HMM framework, and then (iii) the compromised devices will be isolated physically (disconnecting power) and virtually (disconnecting communication) to restore the system. Overall mitigation scenarios will be (1) EVSE is compromised by attackers, (2) disconnecting communication, (3) disconnecting power, (4) disconnecting EV from EVSE, (5) security engineers restore the compromised EVSE, (6) reconnecting communications and (7) re-energizing the power. Similarly, more failure scenarios can arise and different mitigation measures can be implemented depending upon the failure scenario generated by the attack. Also, if the system has prior knowledge of the attack phases, extent of damage and the patching cost can be significantly minimized.

E. Performance of the Proposed Framework

Performance of the proposed framework is highly dependent upon the accuracy of the IDS which can be evaluated in false positive ratio (FPR) and false negative ratio (FNR). It is assumed that IDS can generate either a false negative attack scenario if it doesn't report or emit alerts for each attack event due to misconfiguration, zero-days attacks or a false positive scenario by detecting a non-event. The FPR and FNR of the proposed algorithm depend on the accuracy of the event data and IDS from the XFC station. FPR and FNR are 0.013% and 0.016%, respectively.

F. Comparison of the Novel and State-of-the-Art Algorithms

As shown in Table I, the work of [32] proposes an ADS based on modified bat algorithm to detect the malicious cyber attack behaviors in the CAN traffic, which is highly vulnerable due to the lack of message authentication mechanism.

TABLE I
COMPARISON BETWEEN THE PROPOSED AND THE STATE-OF-THE-ART ALGORITHMS

Solutions	Attack detections	Coordinated attacks	Attack predictions	Active mitigations
Proposed methods	Yes	Yes	Yes	Yes
ADS for EV [32], [33]	Yes	No	No	No
IDS for EV charger [34], [35]	Yes	Yes	No	No

A command-level ADS has been designed for identifying the abnormal behaviors in vehicle-road coordinated charging networks of EVs [33]. The work stated in [34] designs a probabilistic cross-layer IDS based on (k-nearest neighbor) k-NN and random forest (RF) machine learning algorithms for detecting spoofing attacks (e.g., GPS falsification) on inter-vehicle communication, which is required for intelligent routing of EVs around a charging station (static or mobile). Similarly, [35] proposes the deep neural network (DNN) and long short-term memory (LSTM) based IDSs to detect DoS attacks in EV charging station. However, the previous works did not contribute towards the prediction and active mitigation of the abnormal behaviors at the EV charging station network, and also did not analyze different coordinated cyber attack scenarios.

VIII. CONCLUSION

This paper proposes the HMM based cyber attack prediction and mitigation strategies that enhance cybersecurity of the EV charging station. The proposed attack prediction and mitigation algorithms can detect the intrusions, anomalies and abnormal behaviors of cyber attackers. It can also predict the attackers next targets and behaviors. Then it can propose predetermined active defense scenarios so the cyber attacks can be minimized and restored. The STRIDE model has been used for the designing of vulnerability assessment, risk analysis and threat modeling. Then the proposed weighted attack defense tree has been used to create a set of cyber attack scenarios as input for the HMM model. In the future work, a cyber-physical hardware-in-the-loop (HIL) testbed may be designed and simulated to test the real-time implementation and evaluation of the proposed framework and generate more real system data (including normal operations and cyber attacks). Furthermore, the testbed studies can be used to quantify cyber-based vulnerabilities as well as associated risks in the charging station environment and to evaluate the effectiveness of the risk mitigations under realistic and sophisticated attack scenarios. It will also be useful to include more industrial communication protocols (e.g., DNP3 and modbus) and time synchronization information (e.g., PPS, PTP, SNTP and IEEE 1588) related cyber attack scenarios in the XFC station.

REFERENCES

[1] S. Habib, M. M. Khan, F. Abbas, L. Sang, M. U. Shahid, and H. Tang, "A comprehensive study of implemented international standards, technical challenges, impacts and prospects for electric vehicles," *IEEE Access*, vol. 6, pp. 13866–13890, 2018.

[2] D. Aggeler, F. Canales, H. Zelaya-De La Parra, A. Coccia, N. Butcher, and O. Apeldoorn, "Ultra-fast DC-charge infrastructures for EV-mobility and future smart grids," in *Proc. IEEE PES Innovat. Smart Grid Technol. Conf. Eur. (ISGT Europe)*, Gothenburg, Sweden, 2010, pp. 1–8.

[3] H. Tu, H. Feng, S. Srdic, and S. Lukic, "Extreme fast charging of electric vehicles: A technology overview," *IEEE Trans. Transport. Electrific.*, vol. 5, no. 4, pp. 861–878, Dec. 2019.

[4] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[6] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2019.

[7] A. N. Bessani, P. Sousa, M. Correia, N. F. Neves, and P. Veríssimo, "The crutial way of critical infrastructure protection," *IEEE Security Privacy*, vol. 6, no. 6, pp. 44–51, Nov./Dec. 2008.

[8] J. Hong, R. Karnati, C.-W. Ten, S. Lee, and S. Choi, "Implementation of secure sampled value (SeSV) messages in substation automation system," *IEEE Trans. Power Del.*, early access, Feb. 23, 2021, doi: 10.1109/TPWRD.2021.3061205.

[9] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014.

[10] R. Zhu, C.-C. Liu, J. Hong, and J. Wang, "Intrusion detection against MMS-based measurement attacks at digital substations," *IEEE Access*, vol. 9, pp. 1240–1249, 2021.

[11] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan. 2019.

[12] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC 61850-based SCADA networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068–1078, Apr. 2017.

[13] Y. Fraiji, L. Ben Azzouz, W. Trojet, and L. A. Saidane, "Cyber security issues of Internet of electric vehicles," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Barcelona, Spain, 2018, pp. 1–6.

[14] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.

[15] A. Bindra, "Securing the power grid: Protecting smart grids and connected power systems from cyberattacks," *IEEE Power Electron. Mag.*, vol. 4, no. 3, pp. 20–27, Sep. 2017.

[16] D. T. Hoang, P. Wang, D. Niyato, and E. Hossain, "Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: A cyber insurance-based model," *IEEE Access*, vol. 5, pp. 732–754, 2017.

[17] S. Bai and S. M. Lukic, "Unified active filter and energy storage system for an MW electric vehicle charging station," *IEEE Trans. Power Electron.*, vol. 28, no. 12, pp. 5793–5803, Dec. 2013.

[18] S. Rivera and B. Wu, "Electric vehicle charging station with an energy storage stage for split-DC bus voltage balancing," *IEEE Trans. Power Electron.*, vol. 32, no. 3, pp. 2376–2386, Mar. 2017.

[19] N. Machiels, N. Leemput, F. Geth, J. Van Roy, J. Büscher, and J. Driesen, "Design criteria for electric vehicle fast charge infrastructure based on flemish mobility behavior," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 320–327, Jan. 2014.

[20] J. Halvorsen, J. Waite, and A. Hahn, "Evaluating the observability of network security monitoring strategies with TOMATO," *IEEE Access*, vol. 7, pp. 108304–108315, 2019.

[21] Y. Lee, S. Woo, Y. Song, J. Lee, and D. H. Lee, "Practical vulnerability-information-sharing architecture for automotive security-risk analysis," *IEEE Access*, vol. 8, pp. 120009–120018, 2020.

[22] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Commun. ACM*, vol. 57, no. 2, pp. 31–35, Feb. 2014.

[23] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *Proc. IEEE PES Innovat. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Turin, Italy, 2017, pp. 1–6.

[24] P. Danielis, M. Beckmann, and J. Skodzik, "An ISO-compliant test procedure for technical risk analyses of IoT systems based on STRIDE," in *Proc. IEEE 44th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Madrid, Spain, 2020, pp. 499–504.

[25] S. Lightman and T. Brewer, "Symposium on federally funded research on cybersecurity of electric vehicle supply equipment (EVSE)," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NISTIR 8294, Apr. 2020.

[26] D. C. K. Harnett, B. Harris, and G. Watson, "DOE/DHS/DOT volpe technical meeting on electric vehicle and charging station cybersecurity," U.S. Dept. Transp., Washington, DC, USA, Rep. DOT-VNTSC-DOE-18-01, Mar. 2018.

[27] B. Xu, Z. Zhong, and G. He, "A minimum defense cost calculation method for attack defense trees," *Security Commun. Netw.*, vol. 8870734, pp. 1–12, Aug. 2020.

[28] C.-W. Ten, C.-C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for scada systems using attack trees," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Tampa, FL, USA, 2007, pp. 1–8.

[29] "Electric sector failure scenarios and impact analysis," Elect. Power Res. Inst. (EPRI), Washington, DC, USA, NESCOR Rep. version 3, Dec. 2015.

[30] P. Holgado, V. A. Villagrá, and L. Vázquez, "Real-time multistep attack prediction based on hidden Markov models," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 1, pp. 134–147, Jan./Feb. 2020.

[31] M. A. R. A. Amin, S. Shetty, L. Njilla, D. K. Tosh, and C. Kamhoua, "Hidden Markov model and cyber deception for the prevention of adversarial lateral movement," *IEEE Access*, vol. 9, pp. 49662–49682, 2021.

[32] O. Avatefipour *et al.*, "An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning," *IEEE Access*, vol. 7, pp. 127580–127592, 2019.

[33] Q. Li, S. Meng, S. Wang, J. Zhang, and J. Hou, "CAD: Command-level anomaly detection for vehicle-road collaborative charging network," *IEEE Access*, vol. 7, pp. 34910–34924, 2019.

[34] D. Kosmanos *et al.*, "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Array*, vol. 5, pp. 1–11, Mar. 2020.

[35] M. Basnet and M. H. Ali, "Deep learning-based intrusion detection system for electric vehicle charging station," in *Proc. 2nd Int. Conf. Smart Power Internet Energy Syst. (SPIES)*, Bangkok, Thailand, 2020, pp. 408–413.