2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) | 978-1-6654-1779-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/CAMAD52502.2021.9617787

On the Impact of Data Integrity Attacks on Vehicle-to-Microgrid Services

Ahmed Omara, *Student Member, IEEE*, and Burak Kantarci, *Senior Member, IEEE*

***Abstract*—With the increasing demands on the power grid, more Electric Vehicles (EVs) will be used as mobile storage units to trade energy and avoid power shortages. The integration of EVs and smart grids has expanded the attack surface and paved the way for adversaries to perform novel and intelligent attacks on the system. Therefore, data integrity attacks in modern smart grids are expected to increase in Vehicle-to-Grid (V2G) and Vehicle-to-Microgrid (V2M) applications. In this paper, we propose a novel scheme to model data integrity attacks in V2M applications. By leveraging unsupervised machine learning, we implement an intelligent detector to encounter the data integrity attacks. Although some of the data integrity attacks are able to deceive the detector, they fail to impact the V2M service operation. Through simulations, we show that performing the data integrity attacks against an increasing number of EVs (i.e. backup energy suppliers) results in reducing the attacks' impact by up to 76.5%. In addition, doubling the original contribution of EVs alleviates the impact of the data integrity attacks by 60%. On the contrary, doubling the number of microgrids (i.e. demand) raises the attacks' impact by at least 75%.**

***Index Terms*—data integrity attacks, vehicle-to-microgrid, machine learning, smart microgrids**

I. Introduction

The modern power grids are expected to be developed as cyber-physical systems (CPSs) to distribute power flow and transmit data for advanced monitoring and control applications, according to the IEEE Grid vision [1]. In order to enable high efficiency and reliability, modern power grids are heavily dependent on communication devices. Power grids that are improved using bidirectional flow of data and electricity are expected to form smart grids. Emerged features such as demand response, self-recovery and V2G are enabled by smart grids. Energy generated from the Distributed Generators (DGs), such as solar panels and wind turbines, can be shared among other entities connected to the grid, forming Community Resilience Microgrids (CRMs) [2]. The purpose of CRMs is to enhance the availability and sustainability of the delivered power, especially when the main grid is unavailable due to natural disasters and severe weather conditions. Hence, in order to sustain the CRM's goals amid power outages, the concept of energy trading, which we refer to as Vehicle-to-Microgrid (V2MG, a.k.a V2M), builds on utilizing the EV batteries as mobile energy units.

Recent research aims at maximizing the V2G efficiency of the delivered power while reducing the cost using various approaches. For instance, recently the study in [3] has proposed a V2G cost-objective optimization model that aims at finding the closest EVs to a microgrid considering the communication aspects. Similarly, the authors in [4] present a Mixed Integer Linear Programming (MILP) optimization model to minimize the operational cost of the microgrids and the charging cost of the EVs. In addition to optimization models, machine learning techniques such as Reinforcement Learning (RL) was used in power management for grid-tied microgrid problems where V2G service is considered as an alternative power source [5]. Another study models the interactions between the EVs and microgrids where the suppliers (i.e. EVs) specify the plug-in length, arrival times and the amount to supply/sell [6].

Although the cyber-security threats of those V2M interactions have not been studied, some of the existing research efforts investigated the cyber-attacks against the delivery and transmission of data in vehicular networks. For instance, the authors in [7] use an active control concept to detect a special type of data integrity attack, namely False Data Injection (FDI) attacks in a vehicle platoon. A data trust framework is proposed to verify the trustworthiness of the data in the moment [8]. However, the impacts of data integrity attacks against V2M applications have not been systematically investigated.

To the best of our knowledge, for the first time, this paper analyzes the impact of data integrity attacks on smart microgrids. It is assumed that the adversary launches the data integrity attacks on the EVs side, targeting the contribution value as a key parameter. The main contributions are as follows:

- Define a threat model based on the proposed framework in [3] in a V2M setting.
- Provide an in-depth analysis to the risk associated with the modeled attacks on the energy trading processes.
- Understand the effectiveness of intelligent detectors by implementing the proposed attack in the presence of an unsupervised machine learning-based anomaly detector.

The rest of the paper is organized as follows. Section II explains the V2M framework and defines the threat model. Section III models the data integrity attack on the V2M application, and defines the implemented machine learning technique for attacks detection. Section IV demonstrates performance criteria and numerical results regarding with the proposed approach. Section V concludes the paper and provides future directions.

II. System Model for V2M Services

The threat model builds on the optimization model presented in [3] so it is worth revisiting the implemented optimization model before proceeding with the the threat model.

The authors are with the School of Electrical Engineering and Computer Science at the University of Ottawa, Ottawa, ON, K1N 6N5, Canada. E-mail: {aomar020,burak.kantarci}@uottawa.ca

978-1-6654-1779-2/21/$31.00 ©2021 IEEE

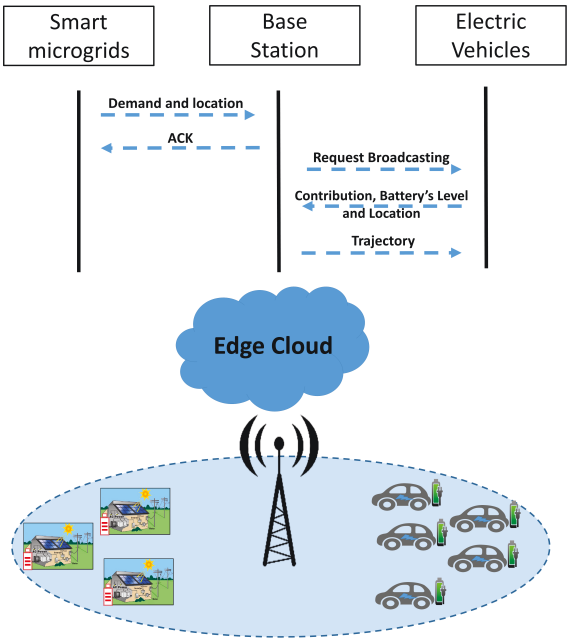


Fig. 1: Message flows in our framework

A. Optimization Model Revisited

The power management framework uses real time information of the microgrid power demand to find the optimal set of EVs to participate in the process, considering reliable communication between the cellular base-station and EVs. The optimization model in [3] is framed as follows: a set of smart microgrids M, that are predicted to suffer from power outage, send highly-time sensitive service requests to the cell's base-station [9]. To ensure reliability, the base-station uses the Transmission Control Protocol (TCP) to acknowledge the reception of the requests [10]. The requests contain information of the anticipated energy demand D_m(kWh) and the microgrid locations. The base-station broadcasts the request to N EVs within the coverage range. Each EV responds to the request with three pieces of information: (i) selling price P_n(\$/kWh), (ii) contribution percentage α_n of the EV's battery E_n, and (iii) current location. Then, the base-station computes the distances between the microgrids K_{im}(km) and chooses an optimal set of EVs to serve the microgrids' requests. Lastly, the base-station sends the trajectories to the EVs, starting with the first microgrid T_m to be serviced. The message flow for the V2M service is depicted in Fig. 1.

The V2M model builds on a MILP formulation to find the optimal set of EVs to supply the affected microgrids with the required power until the main grid is restored. The objective of the optimization problem is to minimize the operational cost especially at the peak hours. Details of this model are presented in [3]; hence the optimization model is explained briefly here. The objective function in (1) can be solved by the set of constraints where (2) and (3) presents the key subset of these constraints. Table I lists the notation used in the MILP model.

TABLE I: Optimization model's notations

Notations	Definition
N	Number of participating EVs in the power supply request
M	Number of microgrids
P_n	Electrical energy price offered by EV n (\$/kWh)
z	Average energy consumption per km (kWh/km)
H	EV's charging power (kW)
C	Waiting cost per hour (\$/h)
v	Constant value defines the cost of the service request made by the microgrid (\$/request)
K_{im}	Distance between microgrid i and microgrid m (km)
T_m	Distance from the initial location of EV n to first microgrid m (km)
E_n	Initial battery level of EV n (kWh)
α_n	Percentage value determines the contribution value of the EV n
S_m^n	Amount of energy that EV n provides to microgrid m (kW)
A_{im}^{nr}	Binary variable defines the multiplication of O_m^{nr} by O_m^{nr+1}
O_m^{nr}	binary variable is one if microgrid m is served by EV n in order r

$$Minimize \sum_{m=1}^{M} cost_m \tag{1}$$

subject to

$$cost_m - (\sum_{n=1}^{N} S_m^n + \sum_{i=1}^{M}\sum_{n=1}^{N}\sum_{r=1}^{M} z \cdot K_{im} \cdot A_{im}^{nr} + \sum_{n=1}^{N} O_m^{n1} \cdot T_m \cdot z) \cdot P_n - (\sum_{n=1}^{N} S_m^n / H) \cdot C - \sum_{n=1}^{N}\sum_{r=1}^{M} O_m^{nr} \cdot v = 0, \forall m \in M \tag{2}$$

The constraint in (3) guarantees that the total transferred energy from EV n and the total consumed energy while traveling does not exceed the contribution factor α of the initial energy level of the EV's battery E_n.

$$\sum_{m=1}^{M} S_n^m + \sum_{i=1}^{M}\sum_{m=1}^{M}\sum_{r=1}^{M} z \cdot K_{im} \cdot A_{im}^{nr} + \sum_{m=1}^{M} O_m^{n1} \cdot T_m \cdot z \leq E_n \cdot \alpha_n, \forall n \in N \tag{3}$$

It is worth mentioning that the communication constraint was excluded from the MILP model to reduce the complexity of the model, as the model has 10 constraints. It is also worth noting that the sole purpose of the aforementioned optimization model is to match sellers (i.e. EVs) with buyers (i.e. smart microgrids) for a V2M application. Detailed version of the optimization model can be found in [3].

B. Threat Model in V2M Services

To understand the threats and possible attacks on V2M application, one should comprehend the involved entities that

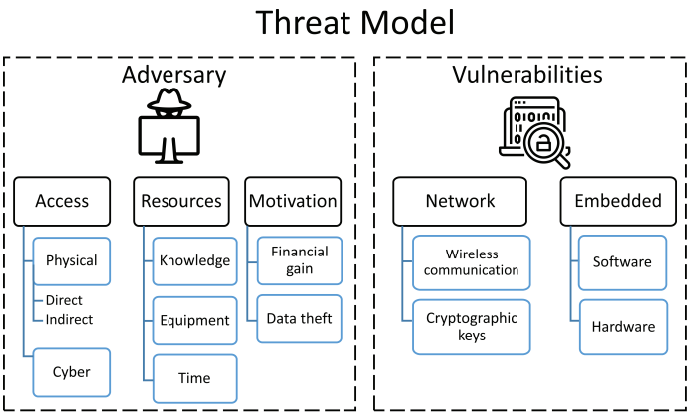


Fig. 2: High-level abstraction of the threat model for V2M

form the threat model. Fig. 2 presents a high level abstraction of the threat model entities including adversaries and vulnerabilities. We conceptually follow the threat model in [11] that is presented for IoT security in smart grids.

1) The adversary represents the first entity of the threat model. The threat level of an adversary is defined by three main elements, namely the required access, the adversary's resources and their motivation.

(i) *Required access:* defines the type of entry point to the network. In order for the adversary to mount an attack, a physical or cyber access to the network is required. Physical-access can be direct through a malicious agent (i.e. an insider) who has privileges in the network, or indirect by an outsider who seeks to gain privileges. It is more likely for attacks to be launched by outsiders who escalate their privileges in the network rather than malicious users, especially in a V2M service, as we will discuss in the performance evaluation section. On the other hand, cyber-access allows the adversary to connect remotely to the network via insecure communication channels. For instance, the adversary can exploit network-based vulnerabilities to gain a full control over the participated EVs during the V2M operation.

(ii) *Required resources:* represent the needed capabilities of the adversary to launch a successful attack. The adversary's resources are defined by the adversary's expertise of the system, the required equipment and time. If the attacker is an expert and aware of the system interactions, it is called a white-box attack. On the contrary, if the attacker is a novice and lacks the necessary knowledge to initiate an attack on the system, it is called black-box attack. In addition, the adversary might need different types of equipment to attack V2M network. For instance, to access an insecure communication channel, the attacker needs to be within the communication range of the traveling EVs, thus, using a vehicle is necessary to launch an attack [12]. However, other attacks might need simpler equipment such as a desktop computer. Another vital resource for the adversary in a V2M application is the amount of time required to perform the attack. The V2M application poses dynamic changes of the network, hence, a dynamic attack surface. Therefore, the adversary has to perform the attack within a limited time window.

(iii) *Motivation:* can be viewed as another definition of the attacker's utility (i.e. the possible gains of performing a successful attack considering the associated efforts and risks to the attacker). Energy and data theft, financial gain, and service disruption are typical examples that drive the adversary [11].

2) The second entity in Fig. 2 is the vulnerabilities in V2M services. There are two parties that form the attack surface in a V2M service, that is, vehicles and smart microgrids. Both parties share network-based and embedded vulnerabilities.

(i) *Network vulnerabilities:* wireless communication and key management expose the network to various types of vulnerabilities. It is worth noting that Autonomous Vehicles (AVs) can be considered as EVs if they use battery units. Thus, network-based vulnerabilities of AVs hold for EVs as well. One of the most commonly used wireless technology for in-vehicle network is Bluetooth. Its ability to hop fast, resist noisy environments and support multi-channel through using Frequency Hopping Spread Spectrum (FHSS) technology made it a favourable technology for Controller Area Network (CAN) communication [13]. However, Bluetooth technology suffers from various vulnerabilities as reported in [12].

(ii) *Embedded system vulnerabilities* are another way for adversaries to break into the EVs. Firmware and operating system vulnerabilities are two main issues for the software-layer of embedded systems. For instance, firmware vulnerabilities allow the attacker to gain full access to the system which can provide the attacker with the control to read and change messages [14] [15]. Moreover, the attacker can pursue and achieve privilege escalation by exploiting operating system vulnerabilities. Hence, the attacker performs the attack seamlessly. Other software vulnerabilities such as in Engine Control Unit (ECU) are possible in [16] whereas embedded hardware in EVs present other exploitable vulnerabilities. The lack of proper hardware implementations and cryptographic algorithms ease the path for adversaries to launch attacks on EVs. Side-channel attacks such as power analysis attacks allow the attacker to extract the encryption keys [17].

III. Modelling of Data Integrity Attack Against V2M Application

We apply the discussed threat model to analyze the impact of the possible security flaws on the V2M operation (i.e. optimization model). We assume an outsider adversary with cyber-access to the system is exploiting in-vehicle communication network using cryptographic key vulnerabilities. The adversary is assumed to be able to alter the messages exchanged between the EVs and the base-station. Hence, we implement a data integrity attack assuming a white-box attack with an expert adversary of the underlying interactions within a V2M service. However, the base-station / edge node is equipped with an intelligent system to detect data integrity attack attempts.

A. Data Integrity Attack

This aim of study is primarily to quantify the impact of cyber-security on energy trading process between EVs and smart microgrids under the presence of an anomaly detector. After analyzing the risks of different parameters involved in the process, we have empirically chosen the contribution value (α_n) to be the best target for an adversary to manipulate. The contribution value is responsible for the amount of traded energy during a V2M service. The adversary's motivation is to weaken the resiliency of smart microgrids community by reducing the amount of provided energy to microgrids (a.k.a buyers). The adversary aims to change the contribution value of the EVs, as it is more susceptible to cyber-attacks. The false contribution values are received at the base-station and used as inputs to the optimization model. However, different false contribution values affect the V2M service differently. For instance, some of the data integrity attacks have zero impact on the service. Thus, we had to assess not only the success of the data integrity attacks but also whether the attacks impacted the service. We define the Impactful Attacks (IA) in formula 4 as the attacks that can bypass DBSCAN and affect the V2M service.

$$IA = \frac{\text{Number of undetected attacks of non-zero impact}}{\text{Total number of attacks}} \tag{4}$$

B. Anomaly Detection

We use DBSCAN to detect the data integrity attack on the V2M application. However, some of the attacks can bypass DBSCAN and impact the V2M services. DBSCAN algorithm is controlled by two parameters, ϵ and $min-points$ where ϵ is responsible for the neighborhood search radius, and the $min-points$ parameter controls the minimum number of points to establish a cluster. The parameters were empirically chosen to make it harder on the adversary to bypass the detector. DBSCAN algorithm works as follows: 1) An initial point is selected and marked as visited. 2) The points within the search radius of epsilon are counted and added to a set. 3) The initial point is considered as a new cluster if the number of points exceeds the predefined min-point value. This process is continued for all points in the neighbourhood. 4) If the number of points is less than the min-point, the point is defined as noise. 5) These steps are repeated until all points are clustered.

DBSCAN has a time complexity of $O(n^2)$ but this can be reduced to $O(nlogn)$ with parameter optimization [18]. Unlike K-means, DBSCAN does not require pre-specification of the number of clusters which makes it a good fit for anomaly detection problems.

IV. Performance Evaluation

A. Simulation Settings

To assess the associated risks of the proposed data integrity attack on the contribution value of the optimization model, Optimization and Simscape Electrical toolboxes are used. All simulations are performed using Intel Core i5-7500 CPU with 16GB of RAM running on a Windows 10 system. The optimization toolbox solves the cost-based MILP model, whereas the Simscape Electrical Toolbox simulates the microgrids and EVs to provide synthetic power data [19]. Table II presents the used simulation parameters.

TABLE II: Simulation parameters

Notations	Value
Number of EVs	$\{6, 12\}$
Number of microgrids (M)	$\{4, 8\}$
Selling price (P_n)	0.201 \$/kWh
Average energy consumption per km (z)	0.18 kWh/km
EV charger's power (H)	20 kW
Waiting time price (C)	10 \$/h
Service request price (v)	1 \$/request
Distance between microgrids (K_{im})	[0.2-3] km
Distance from EV n initial location to first microgrid m (T_m)	[0.2-3] km
Microgrid's demand (D_m)	[5-30] kWh
EV's initial battery level (E_n)	[10-40] kWh
EV's original contribution percentage (α_n)	{20,40,90}%
Reduction percentages of the original contribution	{30,50,70,90}%
ϵ	1.5
$min-points$	5
Number of exploitable EVs for N=6 under 33%, 66% and 100%	2, 4 and 6, respectively
Number of exploitable EVs for N=12 under 33%, 66% and 100%	4, 8 and 12, respectively

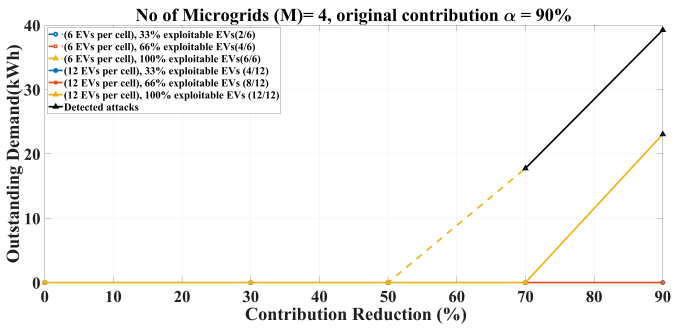
We present two sets of microgrids M=$\{4, 8\}$, where a microgrid's demand (D_m) is picked randomly between [5-30] kWh based on the synthetic power data. Similarly, we consider two scenarios for the number of EVs in the V2M service operation N=$\{6, 12\}$, with different battery levels (E_n) between [10-40] kWh. The adversary targets the contribution value of the EVs. However, the number of exploitable EVs can vary for diverse reasons. Therefore, another objective of this study is to anticipate the number of EVs to be attacked, that would have the heaviest impact on the microgrids' resiliency. Thus, we present three different percentage of EVs that could be exploitable: 33%, 66% and 100%. That is, for N=6, we study the impact of having 2, 4 and 6 exploitable EVs; and for N=12, the number of exploitable EVs is set to 4, 8 and 12. The adversary aims at changing the EVs' contribution values with 100% reduction. However, DBSCAN will prevent that from occurring. After DBSCAN's fine-tuning, we select the ϵ and $min-points$ parameters as 1.5 and 5, respectively.

B. Numerical Results

In this section we analyze the impact of the data integrity attack on the contribution value (α_n) with different number of exploitable EVs. The optimization model has three outputs, outstanding demand (kWh), total cost (\$) and average vehicle's revenue (\$). The outstanding demand defines the amount of the microgrid's energy that could not be supplied by the EVs. The total cost represents the microgrid's cost of exchange for the EVs' energy; and each EV makes a revenue by participating in the request defined by the vehicle's average revenue. For the purpose of this paper, we limit our focus to analyzing the impact of data integrity attacks on the outstanding demand.

(a)

(b)



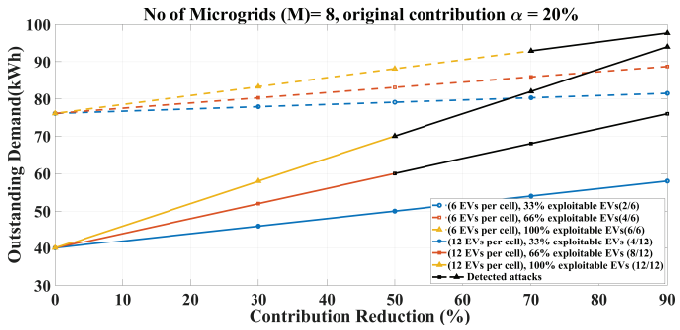
(c)

Fig. 3: Impact of the data integrity attack on the outstanding demand for M=4. (a) original contribution = 20%, (b) original contribution = 40%, (c) original contribution = 90%

1) Analyzing data integrity attacks under four microgrids: The outstanding demand of the 4-microgrid energy request is depicted in Fig. 3a. The EVs are willing to contribute to the request with 20% of their batteries. However, the adversary aims at reducing the original contribution with different percentages as shown on the x-axis. It is important to note that 0% reduction means that the original contribution value has not been changed. In other words, the 0% reduction denotes a "no-attack" case on the V2M operation. We present the no-attack case to show the benign scenario of the model. The dotted-lines represent scenario-1, with six EVs, with different number of exploitable EVs. The solid-lines represent scenario-2, with twelve EVs. The black lines denote the detected attacks by DBSCAN. Under the no-attack case (i.e., 0% reduction), the outstanding demand of scenario-1 is greater than scenario-2. That is because there are more EVs in scenario-2 that can contribute to the request when compared to the number of EVs in scenario-1. Beyond the no-attack point, the effect of the data integrity attacks on the contribution value starts to emerge.

The number of exploitable EVs has different impacts of the outstanding demand. For instance, under the same scenario, the number of attacked EVs is directly proportional to the outstanding demand. The 33% attacked EVs has the least impact on the outstanding demand, whereas the 100% attacked EVs has the highest impact. However, when we compare the two scenarios against each other, one interesting observation from Fig. 3a is that the data integrity attacks on 33% of scenario-1 is more impactful than 100% attacked EVs of scenario-2, for a contribution reduction of 30%. That means attacking two EVs in scenario-1 is more critical and risky to the V2M operation than attacking twelve EVs in scenario-2. This occurs because under the no-attack case, the outstanding demand of scenario-1 is higher than scenario-2. Thus, the six EVs of scenario-1 cannot cover all of the microgrid demands when compared to the twelve EVs scenario, which would have surplus energy even after covering all the demands. Consequently, even with a 30% reduction in the contribution of the twelve EVs in scenario-2, the EVs can still meet the microgrid demands sufficiently. Furthermore, the 30% contribution reduction attack translates into more EV requests to compensate the energy loss caused by the attack. This results in an excessive communication request which will overload the communication infrastructure, especially if those requests are clustered as highly-time sensitive [10]. Moreover, in scenario-2 under 33% attacked EVs, the data integrity attacks have an absolute zero impact on the outstanding demand until a reduction value of 50%. The adversary's utility is negative since the attack has no gains to the adversary. Starting at a reduction of 50% and onward, DBSCAN detects the adversarial attempts on attacking 66% and 100% of the EVs for both cases. That exhibits a promising performance of the applied anomaly detector. However, DBSCAN fails to detect the 33% attacked EVs, for both scenarios, for all reduction percentages. The adversary succeeds to impact the outstanding demand, hence the microgrids' resiliency, by reducing the original contribution value by 70% with attacking 33% EVs of scenario-1.

In Fig. 3b, the EVs' contribution percentage doubles (i.e. 40%) with same number of microgrids M=4. Outstanding demand of the no-attack scenario has dropped when compared to the 20% contribution case. The adversary is successfully able to reduce the original contribution by 30% without being detected for scenario-2. Similarly, for scenario-1, all the data integrity attacks deceived DBSCAN detector except for the 100% exploitable EVs case. At 50% reduction, for scenario-1, the data integrity attack on the 33% exploitable EVs remains undetected, whereas for the other two cases (66% and 100% exploitable EVs), DBSCAN detects the attacks. Beyond the 50% reduction, all the data integrity attacks on the scenario-1 are detected. On the other hand, the data integrity attacks under scenario-2 remain undetected for the 33% and 66% cases until 90% reduction. However, even though the attacks successfully deceived DBSCAN, the attacks have almost zero impact on



(a)

(b)

(c)

Fig. 4: Impact of the data integrity attack on the outstanding demand for M=8. (a) original contribution = 20%, (b) original contribution = 40%, (c) original contribution = 90%

the outstanding demand. Hence, not all successful attacks can impact the V2M operation. Furthermore, that can be seen, as the original contribution increases to 90% as depicted in Fig. 3c. It is worth noting that none of the undetected attacks have any impact on the outstanding demand. In addition, the 100% exploitable EVs case for scenario-1 and scenario-2 are detected successfully. Hence, the performed attacks on an original contribution of 90% have no impact on the V2M operation for both scenarios. That is because the EVs for both scenarios have enough energy to meet the microgrid demands even under different contribution reduction attacks. However, as mentioned earlier, the attacks on the contribution values will result in heavier communication load. Lastly, increasing the original contribution from 20% to 40% results in doubling the detected data integrity attacks of scenario-1.

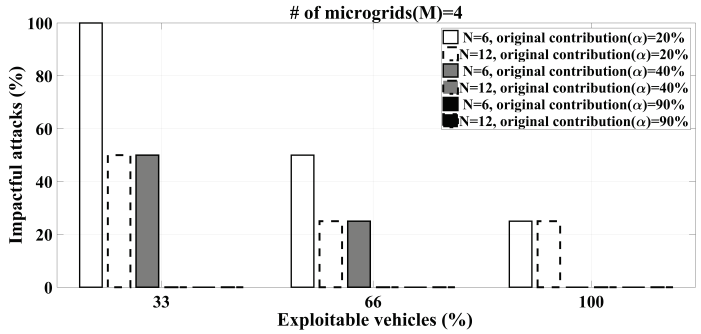
2) Analyzing data integrity attacks under eight microgrids: We also double the number of microgrids (i.e. M= 8) to further investigate its relation to the outstanding demand. In Fig. 4a under 20% original contribution and 8 microgrids, the outstanding demand increases by around 40kWh for both scenarios under the no-attack case (i.e. 0% contribution reduction) when compared to the 4-microgrids case. That means neither the six EVs scenario nor the twelve EVs scenario can sufficiently meet the microgrid demands. Contrary to the 4-microgrids case, the data integrity attack against the 33% exploitable EVs of scenario-2 has impacted the outstanding demand under all different contribution reduction attacks. Hence, it is shown that increasing the number of microgrids has a linear impact on the outstanding demand under 20% original contribution.

On one hand, doubling the original contribution to 40% lowers impact of the integrity attack on the outstanding demand for both scenarios as shown in Fig. 4b. On the other hand, doubling the number of microgrids to 8 results in an increase in the outstanding demand. Hence, the positive impact of increasing the original contribution from 20% to 40% cancels the negative impact of increasing the number of microgrids from 4 to 8. Thus, Fig. 4b could represent 4 microgrids with 20% original contribution (i.e. an exact replica of Fig. 3a). As we further increase the original contribution to 90%, the data integrity attacks lead to a lower impact on the outstanding demand as depicted in Fig. 4c. However, when compared to Fig 3c with M=4 and 90% original contribution, the impact of different exploitable cases under scenario-1 becomes noticeable.

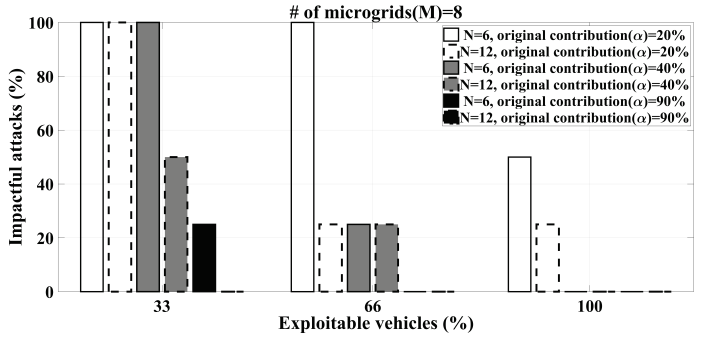
Since not all the data integrity attacks affect the outstanding demand of the V2M operation, we evaluate the impact of the performed attacks on 4 and 8 microgrids as presented in Fig. 5. It is shown that the impactful attacks percentage is affected by four factors: (i) the original contribution (ii) the number of EVs (N) (iii) exploitable EVs percentage (iv) the number of microgrids (M). As the original contribution percentage increases, the impactful attacks either decrease or remain constant. For instance, in 33% exploitable EVs for N=6, the impactful attacks rate drops from 100% to 50% as the original contribution increases from 20% to 40%. Similarly, the impactful attacks rate drops from 100% to 50% as the N grows from 6 to 12 under the same contribution value of 20% and 33% exploitable EVs. Furthermore, increasing the exploitable EVs percentage results in a decrease of the impactful attacks rate when the other factors remain the same.

V. Conclusion

In this paper, we studied data integrity attacks as potential cyber-threats on Vehicle-to-Microgrid (V2M) service operation, in which the adversary alters the original contribution of the EVs. We have modeled and performed an in-depth impact analysis for these threats considering the microgrid demands that could not be covered by the EVs (i.e. the outstanding demand), in a V2M operation. Numerical results have shown that the risk of data integrity attacks on the outstanding demand as well as the impactful attacks rate can drop by



(a)



(b)

Fig. 5: Impactful attacks on the V2M operation for different exploitable EVs (a) M=4 (b) M=8

increasing the original contribution and the number of EVs; the risk rises when the number of exploitable EVs and the number of microgrids increase. For instance, increasing the original contribution from 20% to 90% resulted in dropping the outstanding demand by up to 100% and 93% for the 4 and 8 microgrids cases, respectively. Similarly, rising the number of EVs from 6 to 12 resulted in dropping the outstanding demand by up to 76.5% and 30% for the 4 and 8 microgrids cases, respectively.

Investigation of the overhead on the communication infrastructure as a result of the data integrity attacks on V2M operation, and introducing complex data integrity attacks that take into consideration variables other than the vehicular contribution are in our ongoing research agenda. Furthermore, from the defensive point of view, we are studying different strategies to connect as many as EVs from different cell-tiers (i.e. heterogeneous networks) to reduce the effect of data integrity attacks.

ACKNOWLEDGMENT

This work was supported in part by the U.S. National Science Foundation under Grant CNS-1647135, in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) under the DISCOVERY Program.

REFERENCES

[1] M. Higgins, F. Teng, and T. Parisini, "Stealthy mtd against unsupervised learning-based blind fdi attacks in power systems," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1275–1287, 2020.

[2] J. Zhang, J. Li, L. Wu, M. Erol-Kantarci, and B. Kantarci, "Hierarchical optimal control of the resilient community microgrid in islanded mode," in *IEEE Power Energy Society General Meeting*, 2019, pp. 1–5.

[3] M. Simsek, A. Omara, and B. Kantarci, "Cost-aware data aggregation and energy decentralization with electrical vehicles in microgrids through lte links," in *IEEE Intl Black Sea Conference on Communications and Networking (BlackSeaCom)*. IEEE, 2020, pp. 1–6.

[4] X. Zhaoxia, L. Hui, Z. Tianli, and L. Huaimin, "Day-ahead optimal scheduling strategy of microgrid with evs charging station," in *2019 IEEE 10th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*. IEEE, 2019, pp. 774–780.

[5] A. O. Erick and K. A. Folly, "Reinforcement learning approaches to power management in grid-tied microgrids: A review," in *2020 Clemson University Power Systems Conference (PSC)*. IEEE, 2020, pp. 1–6.

[6] J. Lee and G.-L. Park, "A heuristic-based electricity trade coordination for microgrid-level v2g services," *International Journal of Vehicle Design*, vol. 69, no. 1-4, pp. 208–223, 2015.

[7] R. A. Biroon, P. Pisu, and Z. Abdollahi, "Real-time false data injection attack detection in connected vehicle systems with pde modeling," in *American Control Conference (ACC)*, 2020, pp. 3267–3272.

[8] M. Sun, M. Li, and R. Gerdes, "A data trust framework for vanets enabling false data detection and secure vehicle tracking," in *IEEE Conf. on Communications and Network Security (CNS)*, 2017, pp. 1–9.

[9] A. M. E. Omara, "Predictive operational strategies for smart microgrid networks," Ph.D. dissertation, University of Ottawa, 2020.

[10] A. Omara, B. Kantarci, M. Nogueira, M. Erol-Kantarci, L. Wu, and J. Li, "Delay sensitivity-aware aggregation of smart microgrid data over heterogeneous networks," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–7.

[11] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[12] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & Security*, p. 102150, 2021.

[13] M. Bacchus, A. Coronado, and M. A. Gutierrez, "The insights into car hacking," 2014.

[14] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, "0-days & mitigations: Roadways to exploit and secure connected bmw cars," *Black Hat USA*, vol. 2019, p. 39, 2019.

[15] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to can bus," *Briefing, Black Hat USA*, vol. 25, pp. 1–16, 2017.

[16] S. Shukla, "Embedded security for vehicles: Ecu hacking," 2016.

[17] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "Iot goes nuclear: Creating a zigbee chain reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 195–212.

[18] M. Ester, H.-P. Kriegel, J. Sander, X. Xu *et al.*, "A density-based algorithm for discovering clusters in large spatial databases with noise." in *Kdd*, vol. 96, no. 34, 1996, pp. 226–231.

[19] A. Omara, W. Yuan, M. Nogueira, B. Kantarci, and L. Wu, "Microgrid data aggregation and wireless transfer scheduling in the presence of time sensitive events," in *ACM Intl. Symp. on Mobility Management and Wireless Access*, 2018, pp. 109–112.