电动汽车僵尸网络对电力的影响网格

Omniyah Gul M Khan 、 Ehab El-Saadany † 、 Amr Youssef ‡和 Mostafa Shaaban §
加拿大滑铁卢大学电气和计算机工程 †阿联酋哈利法大学 EECS 系高级电力和能源中心和 ECE 兼职教授加拿大滑铁卢大学系 ‡加拿大康考迪亚大学康考迪亚信息系统工程学院 §阿联酋沙迦美国大学电气工程系

摘要:随着电动汽车 (EV) 在交通运输领域的普及,对快速充电直流 (FCDC) 站的需求也随之增加,以满足客户的快速充电需求。然而,充电站和电动汽车都连接到通信基础设施和电网,使其容易受到网络攻击。本文初步研究了电动汽车充电过程的脆弱性。然后,我们展示了如何利用受感染的电动汽车和 FCDC 站组成的僵尸网络对电网发起网络攻击,从而导致特定时间的负载增加。研究了此类攻击在线路拥塞和电压限制违规方面对配电网络的影响。此外,还研究了传输网络僵尸网络的影响。仿真结果证明了线路故障和停电的可能性;因此,建立了系统对网络攻击的脆弱性。

一、引言

电动汽车 (EV) 部署的增加增加了对公共快速充电站的需求。目前,基于 SAE J1772 标准 [1],以下三种主要充电方式用于住宅、商业或公共环境:

- 慢速充电 1 级:主要是住宅充电器,在-120V 时最大电流为 16 安培的车载充电器。根据 EV 的电池技术,1 级充电需要 8 到 12 小时才能为空电池充满电。
- 2 级标准充电:通常在住宅或商业上以 240V 的最大 80 安培速率向 EV 车载充电器提供交流能量。根据 EV 的电池技术,2 级充电需要 4 到 6 小时才能为空电池充满电。
- 3 级快速充电:通常在商业上或高速公路上使用,从车外充电器向电动汽车提供直流能量。目前最常见的 3 级充电器形式提供每小时 50kW 的充电量。另一方面,特斯拉 3 级充电器每小时可提供 120kW 的电量。

随着电动汽车日益流行,中低阶层家庭也能负担得起。

然而,并非所有电动汽车消费者都拥有自己的住宅物业来为汽车充电。相反,他们中的许多人可能还活着在更密集的环境中,需要安装公共 2 级或 3 级充电站以满足其充电需求。此外,为了吸引更多人驾驶电动汽车,未来将部署大规模快速充电直流 (FCDC) 站,提供快速充电。然而,电动汽车和充电站都被视为物联网 (IoT) 设备,因为它们通过互联网相互连接。因此,电动汽车和充电站的网络安全在其设计和电网集成中发挥着重要作用。此外,相关的电动汽车充电通信标准还处于起步阶段,不够开放,默默无闻迫使安全性。

网络攻击者可以创建一个由受感染的电动汽车和充电站组成的网络,称为僵尸网络,以对电网造成更大的影响(僵尸网络是由僵尸主机远程控制的可控设备网络,以进行网络攻击 [2])。就负载的未考虑增加而言,尤其是在高峰时段,电动汽车的充电已经引起了人们的关注。如果攻击者决定创建一个利用僵尸网络进一步大幅增加电网负载的场景,那么 EV 僵尸网络可能会对电网造成巨大影响,很可能会导致电网中断。本文将研究这种 EV 僵尸网络攻击对配电和传输网络的影响。

现代汽车网络安全的研究基本上是在 2010 年左右开始的。在 [3] 中,研究了汽车的外部攻击面。针对汽车的电子控制单元 (ECU) 实施了不同的攻击。攻击者能够利用易受攻击的汽车的外部 I/O 接口来远程控制各种车辆功能。在 [4] 中,使用连接的车辆实施无线攻击,其中驾驶员的电话连接到车辆的控制器局域网 (CAN)。最初,假设攻击者已获得对汽车局域网 (CAN) 数据帧的访问权限以控制车辆。此外,假设攻击者发布了一个恶意应用程序,当驱动程序下载它时,攻击者可以通过该应用程序控制驱动程序的手机。此外,基于[5],充电站基础设施对潜在的网络攻击是开放的,因为它们是无人驾驶的并且偶尔位于偏远地区。另一方面,[6] 和 [7] 表明,高功率设备的 IoT 僵尸网络为攻击者提供了

操纵电网需求导致停电和/或停电的能力。索尔坦等人。 [8] 提供了防止由于这种需求操纵而导致线路故障的方法。

然而,据我们所知,以前没有研究过由电动汽车和充电站组成的僵尸网络对输配电网络的影响。

本文的主要贡献有两个:(1)评估电动汽车充电过程的脆弱性;(2)模拟对配电网和输电网络的网络攻击,并研究其对拥塞、线路故障和中断的相应影响.

二、电动汽车充电漏洞分析

任何网络安全系统都应具备的基本特征由 CIA 三元组 [9] 表示,它象征着机密性、完整性和可用性。需要保密以确保对敏感信息的访问受到限制和授权。另一方面,完整性是指确保信息真实且未损坏。

最后,可用性是授权用户随时可以访问所需信息和服务的保证。因此,电动汽车充电的成功取决于网络网络的中央情报局,如果不解决安全漏洞,可能会对智能电网构成重大威胁。

利用 EV 与充电站的物理连接和通信连接,先前的研究已经揭示了网络攻击者在为 EV 充电的过程中可以利用的几个漏洞来源 [10]、[5]、[11]。这些漏洞总结如下(另请参见图 1):

·当需要加油时,EV 用户通过移动应用程序与与其有合同的移动服务提供商 (MSP) 进行通信,以确定最近的可用充电站。攻击 MSP 可以允许访问个人 EV 驾驶员和车辆信息,将 EV 驾驶员引导至繁忙的充电站,显示所需充电站不可用,迫使 EV 车主驾驶更昂贵的充电选项 (FCDC),或影响计费和支付消耗

活力。

· EV 和充电站之间通过充电电缆的连接器端口交换信息。

充电状态 (SOC) 最初由 EV 与 EV 电池的电压范围和载流量一起传送到充电站 [12]。如果电动汽车感染了恶意软件,充电站也可能受到感染,恶意软件可能会传播到未来使用同一充电站加油的其他电动汽车。

电动汽车的移动性也可用于将恶意软件传播到其他充电站。 ·攻击充电站本身会导致电动汽车无法充电到所需的SOC,即攻击者可以停止对电动汽车充电。攻击者还可以让电动汽车免费充电。此外,攻击者可以忽略 EV 电池的载流量限制,并以超出 EV 容量的速率充电,从而对 EV 造成故意损坏。

·充电站运营商 (CPO) 负责运营和维护一系列充电站。

当用户到达充电站时,MSP 验证用户,然后 CPO 能够开始充电过程。攻击 CPO 可能导致向 EV 提供错误的充电量,甚至在未达到用户要求的情况下停止充电过程, ·网络攻击者可以实施中间人攻击并拦截甚至更改 EV 和充电站、EV 和 MSP、MSP 和 CPO,或 CPO 和充电站 [13]。

图 1. 电动汽车充电过程中的网络漏洞

利用这些漏洞中的任何一个都可能产生毁灭性的影响。在本文中,充电站和电动汽车受到攻击,形成了一个僵尸网络,增加了电网负载。然而,本文没有考虑拒绝服务攻击、窃电和侵犯隐私等攻击[14] [15]。

三、 EV僵尸网络对分销网络的影响

为了研究 EV 僵尸网络对配电网络的影响,使用了 IEEE 33 总线网络 [16],如图 2 所示。 32 个负载总线的非灵活基本负载配置文件被设计为等效于 IEEE 33 总线系统的默认负载 [16]。所有负载总线,除了总线 24,被假定为住宅,由 EV 和热泵 (HP) [17] 作为灵活负载。巴士 24 具有最大的基本负载,代表一辆商业巴士,由一个可容纳 50 辆电动汽车的电动汽车快速充电停车场组成。

从多伦多停车管理局 [18] 获得的数据表示商业区停车场中电动汽车的到达和离开时间,用于模拟 24 路公交车停车场中电动汽车的可用性。每辆电动汽车的初始充电状态 (SOC) 为随机均匀分布在 20% 和 30% 之间,并且假设车主希望汽车

表一
案例研究参数

多变的	价值
性能系数 (COP)	2.2
住宅区	1500-2500 平方英尺
房屋温度范围	18-24°C
电动汽车电池尺寸	36 kWh
最大住宅电动汽车充电功率	11 kW
最大快速充电电动汽车功率	50 kW
EV初始SOC	0.2-0.3
支路 1-2 的潮流限制	7.91 MW
电压上限	1.05 pu
电压下限	0.95 pu

出发时完全收费。模拟 HP 和 EV 运行以及执行潮流分析所需的各种参数列于表 I。

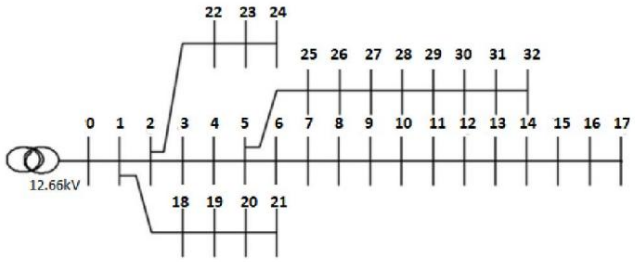

图 2. IEEE 33 总线系统用作配电网络案例研究 [16]

此外,假设快速充电站被放置在一些住宅公共汽车上,供居住在缺乏家庭充电站所需空间的多住宅单元中的消费者使用。 MATPOWER [19] 用于模拟 IEEE 33 总线网络的基本情况,以确定网络中最大电压降的最薄弱点。在进行潮流分析后,观察到母线 17 和母线 16 的母线电压最低。因此,假设攻击者知道她正在攻击的网络,则假设有 50 个 FCDC 站位于这两条总线上。图 3(a) 说明了 IEEE 33 系统分支 0-1 中具有和不具有灵活负载的功率流量。正如所观察到的,没有拥塞,因为并非所有 FCDC 都在同一时刻运行。然而,当攻击者利用 EV 僵尸网络并在 07:00 时间将所有需要充电的 EV 引导至 FCDC 充电站时,随着所有 FCDC 站的运行,对电力的需求会增加。这种攻击是一种负载改变攻击[20],它会导致电网拥塞,如图 3(b) 所示,其中分支 0-1 中流动的功率超过了其容量。配电网络运营商 (DNO) 将要求立即卸载或分支 0-1 发生线路故障,从而导致停电。

由于 FCDC 点位于母线 16 和 17 的两个最弱电压点,因此在图 4 中可以清楚地看到对电压的影响。由于 07:00 的网络攻击,当时的最低电压降至以下NEC 5% 电压降建议。因此,需要在网络中实施任一电压支持方法

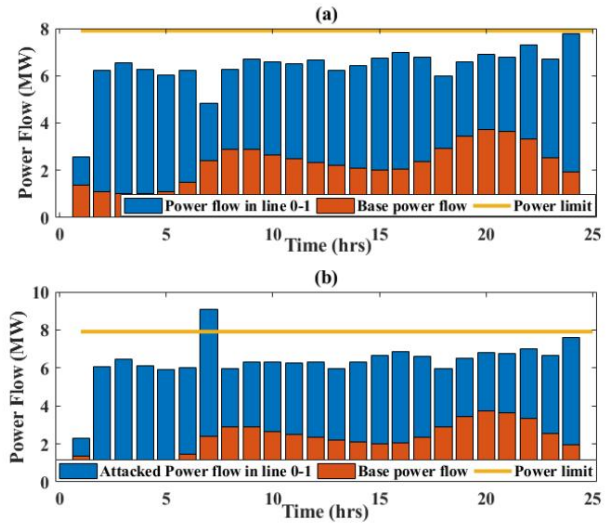

图 3. EV 僵尸网络攻击对 0-1 线负载的影响 其中 (a) 表示正常运行的潮流， (b) 表示网络攻击导致的潮流

会产生成本或提供给消费者的电压不会达到额定电压,从而导致负载不正常、不稳定或不运行,并最终损坏设备。此外,由于高电阻连接处潜在的火灾危险,过压降也是一个问题。

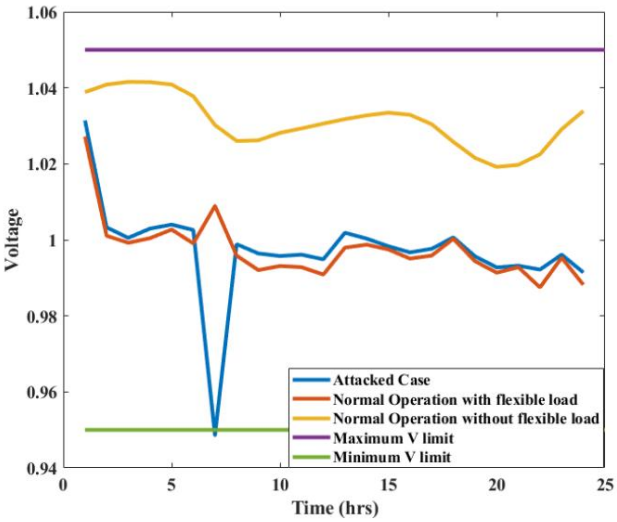

图 4. EV 僵尸网络网络攻击对最低总线电压的影响

四。电动汽车僵尸网络对传输网络的影响

通常在配电网络级别观察到负载更改攻击。但是,可以通过在传输级别研究系统来理解这种攻击的影响。

因此,为了研究 EV 僵尸网络对传输网络的影响,使用了 IEEE 39 [21] 总线系统,该系统由 39 个总线、10 个发电机和 46 个分支组成,如图 5 所示。

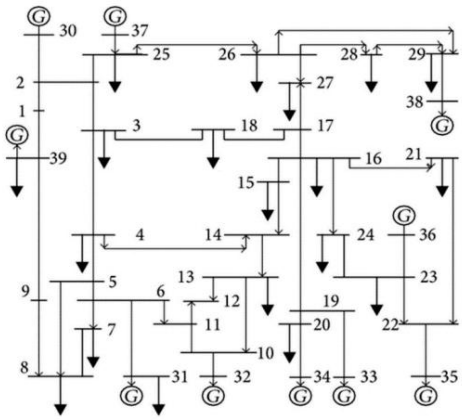

图 5. IEEE 39 总线系统用作传输网络案例研究 [21]

IEEE 39 总线系统有 19 条负载总线。为了模拟利用 EV 僵尸网络的网络攻击,这些总线上的负载增加了 5%。例如,母线 20 的基本负载为 680MW。因此,增加 5% 对应于增加 34MW,这代表 680 个 FCDC 点同时运行以为电动汽车充电。为了不触发配电网络中的保护系统,负载总线的增加不应导致其各自网络的任何拥塞。 IEEE 39 总线系统的总线 9 的负载为 6.5MW,对应于上一节中解释的 IEEE 33 总线系统的 19:00 时刻的负载。

因此,在 19:00 时有负载的 IEEE 33 总线系统被用来模拟 IEEE 39 总线系统的总线 9 上的负载。
最初,在没有攻击的情况下,根据从多伦多停车管理局 [18] 获得的数据,模拟了 24、17 和 16 路公交车上的 5 个 FCDC 点,其中电动汽车正在充电。进行潮流分析,得到支路 0-1 的潮流,观察是否有拥塞。然后触发网络攻击,导致所有 5 个 FCDC 点在 19:00 时间充电。图 6 描述了即使攻击发生在 19:00 时也没有拥塞,导致负载增加 6.5%。因此,不会触发配电级别的保护系统。

当使用 19:00 的负载来研究这种攻击对传输系统的影响时,在执行潮流分析时,观察到连接总线 15 和 14 的分支 24 过载。该分支被停用,网络仍然完整,没有观察到存在孤立的岛屿。重新执行潮流分析导致连接母线 18 和 3 的支路 7 过载。该支路也被停用,网络仍然完整,没有观察到存在孤立的孤岛。重复潮流分析,导致连接母线 27 和 17 的支路 31 和连接母线 26 和 25 的支路 31 过载。这导致创建三个岛:岛 1 由 23 个支路、5 台发电机和 20 台母线组成。岛 2 由 14 辆公共汽车、4 台发电机和 14 辆公共汽车组成。 3 号岛由 5 个分支、1 台发电机和 5 辆公共汽车组成。此外,即使我们的线路由于过载而停用,系统仍然能够提供所有负载。因此,没有观察到停电。

但是,将所有负载总线上的负载增加 10% 会导致中断。最初,确保负载总线的这种增加不会导致配电系统发生任何拥塞而触发其保护系统。使用 IEEE 33 总线系统作为负载为 6.5MW 的 IEEE 39 总线系统的总线 9 的负载,重复前面解释的相同过程。在没有发生攻击的情况下,根据从多伦多停车管理局获得的数据,模拟了 24、17 和 16 路公交车上的 10 个 FCDC 点,其中电动汽车正在充电。执行潮流分析以确定支路 0-1 中的功率流动,并观察是否会出现拥塞。然后触发网络攻击,导致所有 10 个 FCDC 点在 19:00 时间充电。

图 7 说明了即使在 19:00 发生攻击导致负载增加 11.8% 时,配电网络也没有出现拥塞。因此,不会触发配电级别的保护系统。

然后使用 19:00 的负载研究此类攻击对传输系统的影响,观察到 4 个分支过载。这些分支被停用,网络仍然完整,没有观察到存在孤立的岛屿。重新执行潮流分析会导致 9 个分支过载,当停用时会导致创建 9 个孤岛。由于负载母线 13 和 4 被隔离且无法提供,因此该过程继续导致 16 个支路过载和 559.4MW 的停电（占原始负载的 8%）。图 8 使用虚线说明了停用的分支,红色框表示隔离的负载总线。

五、结论

本文研究了网络攻击者利用由 EV 和 FCDC 站组成的僵尸网络攻击电网的影响。初步研究了EV充电过程的脆弱性,并使用IEEE 33总线系统演示了使用EV增加负载的效果

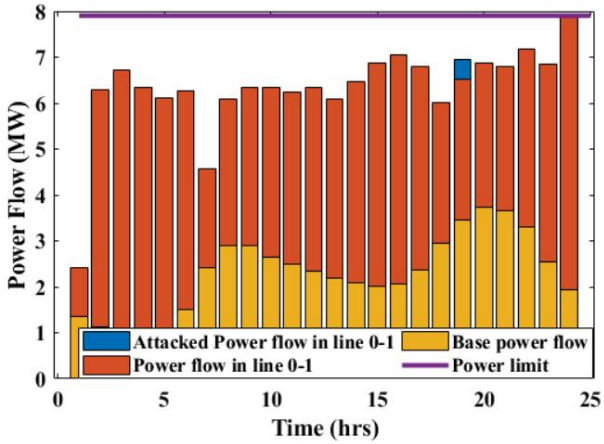

图 6. 由 5 个 FCDC 站组成的 EV 僵尸网络对 0-1 线负载的影响,其中 (a) 代表正常运行的潮流,(b) 代表由网络攻击

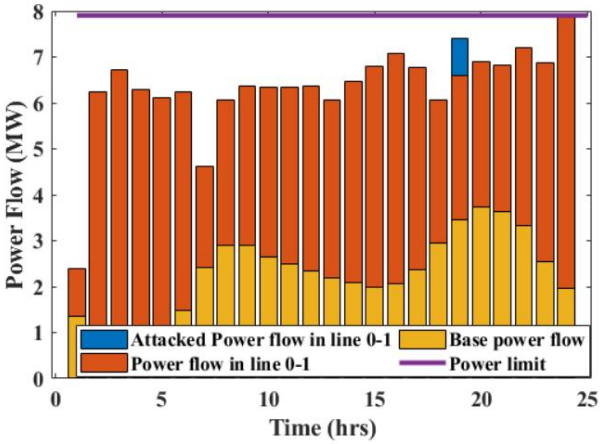

图 7. 由 16、17 和 24 路旁 10 个 FCDC 站组成的 EV 僵尸网络对 0-1 线负载的影响 其中 (a) 代表正常运行功率流,(b) 代表功率流网络攻击

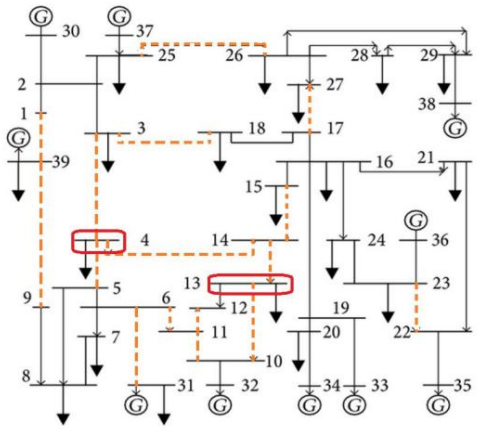

图 8. 由于僵尸网络网络攻击导致线路过载而形成的两条静载总线将所有总线的负载增加 10%

配电网络上的僵尸网络导致线路拥塞和电压限制违规。此外,攻击者可以增加负载,使得配电网络的保护系统没有被触发,但在传输网络中观察到攻击的影响是在中断方面。因此,电动汽车和 FCDC 站的安全性对于电网的安全可靠运行至关重要。需要进一步研究调查对多个充电站的协同攻击对系统电压和频率的影响。

此外,需要开发检测和保护系统免受此类攻击的预防方法。

参考

[1] Y. Kongjeen、W. Junlakan、K. Bhumkittipich 和 M. Nadarajah,“基于位置和人口密度数据的电动汽车快速充电站估算”,国际智能工程与系统杂志,第一卷。 11,第 233-241 页,2018 年 6 月。

[2] L. Cao 和 X. Qiu,“防御僵尸网络:正式定义和通用框架”,2013 年 IEEE 第八届网络、架构和存储国际会议,2013 年 7 月,第 237-241 页。

[3] S. Checkoway、D. McCoy、B. Kantor、D. Anderson、H. Shacham、S. Sav age、K. Koscher、A. Czeskis、F. Roesner 和 T. Kohno,“综合实验分析汽车攻击面”,第 20 届 USENIX 安全会议论文集,ser。 SEC 11。美国加利福尼亚州伯克利:USENIX 协会,2011 年。

[4] S. Woo、HJ Jo 和 DH Lee,“对联网汽车和车载安全协议的实用无线攻击”,IEEE Transactions on Intelligent Transportation Systems,第一卷。 16,没有。 2,第 993-1006 页,2015 年 4 月。

[5] C. Hille 和 M. Allhoff,“电动汽车充电:为电网和充电基础设施绘制网络安全威胁和解决方案”,UtiliNet Europe,2018 年 5 月。

[6] S. Soltan、P. Mittal 和 HV Poor,“Blackiot:高功率设备的物联网僵尸网络可以破坏电网”,USENIX 安全研讨会,2018 年。

[7] A. Dabrowski、J. Ullrich 和 E. Weippl,“电网冲击:对电网的协调负载变化攻击:非智能电网也容易受到网络攻击”,2017 年 12 月,第 303- 314.

[8] S. Soltan、P. Mittal 和 HV Poor,“保护电网免受高功率设备的物联网僵尸网络攻击”,计算研究资料库,2018 年。

[9] M. Vai、B. Nahill、J. Kramer、M. Geis、D. Utin、D. Whelihan 和 R. Khazan,“嵌入式系统的安全架构”,2015 年 IEEE 高性能极限计算会议 (HPEC),2015 年 9 月,第 1-5 页。

[10] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui,“车联网的攻击与对策, ” 电信年鉴,第一卷。 2016 年 72 月 11 日。

[11] S. Fries 和 R. Falk,“电动汽车充电基础设施 安全考虑和方法”,国际互联网发展会议,2012 年 6 月。

[12] Hydro-Quebec,“电动汽车充电站技术安装指南”,Tech。众议员,2015 年。

[13] HBCD Harnett、Kevin 和 G. Watso,“Doe/dhs/dot volpe 电动汽车和充电站网络安全报告技术会议”,
技术。众议员,2017 年。

[14] MA Mustafa、N. Zhang、G. Kalogridis 和 Z. Fan,“智能电动汽车充电:安全分析”,2013 年 IEEE PES 创新智能电网技术会议 (ISGT),2013 年 2 月,第 1-6 页.

[15] RM Pratt 和 TE Carroll,“车辆充电基础设施安全”,2019 年 IEEE 国际消费电子会议 (ICCE),2019 年 1 月,第 1-5 页。

[16] ME Baran 和 FF Wu,“配电系统中的网络重构以减少损耗和负载平衡”,IEEE Transactions on Power Delivery,第一卷。 4,没有。 2,第 1401-1407 页,1989 年 4 月。

[17] W. Liu、Q. Wu、F. Wen 和 J. Ostergaard,“通过家庭需求响应和配电拥塞价格对配电系统进行日前拥塞管理”,IEEE Transactions on Smart Grid,第一卷。 5,没有。 2014 年 11 月 6 日。

[18] EA Rezai、M. Shaaban、E. El-Saadany 和 F. Karray,“通过插入式电动汽车的交互式整合来响应需求”,2015 年 IEEE 电力能源协会大会,2015 年,第 1- 5.

[19] RD Zimmerman、CE Murillo-Sanchez 和 RJ Thomas,“Matpower:用于电力系统研究和教育的稳态操作、规划和分析工具”,IEEE Transactions on Power Systems,第一卷。 26,没有。 1,第 12-19 页,2011 年 2 月。

[20] OGM Khan、E. El-Saadany、K. Saleh、M. Shaaban 和 A. Youssef,“分布式拥塞管理方法的网络攻击”,2019 年 IEEE PES 大会,2019 年接受。

[21] T. Athay、R. Podmore 和 S. Virmani,“一种直接分析暂态稳定性的实用方法”,IEEE Transactions on Power Apparatus and Systems,第一卷。 PAS-98,没有。 2,第 573-584 页,1979 年 3 月/4 月。