电动汽车和充电站技术作为漏洞威胁和黑客崩溃智能电网

赛义德·艾哈迈德

国际工程技术最新发展大会 (RDET-16) 8 月 22 日-
2016 年 2 月 24 日,吉隆坡（马来西亚）

电动汽车和充电站技术作为漏洞威胁和黑客破坏智能电网

S.Ahmed,调频陶氏

摘要近年来,执行数量的攻击是为了提高电力系统知识,可能能够创建一个
诚信遍天下。明智地 充电站的安全发展成为当务之急。智能电网的关注和集成不同技术的道路上电动汽车的质量越来越有趣。例如,充电点是智能电网的一部分。极大地增加了内部充电点其他功能的巨大风险,必须保护其免受外部连接的影响,它对智能电网产生负面影响,网络攻击正在迅速增加。网络恐怖分子正在寻找新的组件以确保对其进行保护,有必要在恐怖分子或其他对手能够利用它们之前检测关键系统中的漏洞。通过网络手段攻击其无线控制系统,破坏被认为是每项活动骨干的电力基础设施,已成为削弱能源系统平台网络攻击的重要途径。在本文中,我们提供充电站作为攻击恶意程序和其他攻击能源网络的平台,这个概念解释了如何使用充电站

配备所有技术连接和软件的充电站技术利用管理能量对敏感区域进行攻击,攻击旨在通过向智能电网发送无限的虚假请求来利用资源。作为研究论文的一部分,我们进一步细分了用于通信和应用基础设施的充电站技术。另一方面。我们介绍了充电站基础设施针对智能电网系统中的漏洞威胁和黑客崩溃的背景和动机。由于智能电网系统可能容纳数百万个不安全的充电点和电动汽车,我们进一步探索了作为复杂智能电网系统一部分的无线通信和应用基础设施的充电站技术。

索引词 充电点、脆弱性、智能电网、通信技术。

一、引言

智能电网技术是机器对机器 (M2M) 的一种范式,被定义为用于下一代通信的新技术,其中大量智能机器共享信息并协作做出决策,而无需人工干预。对电动汽车基础设施的需求更大。随着道路上的电动汽车（EV)的数量越来越多。重要的制造商之一是无线技术。有充电

S.AHMED,高等技术学院,Regdleen,利比亚 FM Dow 利比亚研究、科学和技术管理局,利比亚的黎波里）。

站和他在世界上的现场充电器。公共充电站至关重要,此类充电站有助于扩大电动汽车的电动续航里程。因此,电动汽车运营商的数量将会增加,并使他们更适合长途旅行。 , 这个智能电网将是建立一个足够密集的充电站网络所必需的,这些都是部署充电站所必需的,这些充电站可以位于任何位置,在机场、购物中心,以及控制较少的地方,如路边、路边或路边高速公路[2]。

基础设施的智能通信将电动汽车与电动汽车供应设备 (EVSE) 联系起来。 EVSE 单元通常被称为“充电站”。提供了一种交换此类基本信息的敏感方式,这种组合在未来可用于能源交易、投标和更多对高级智能电网应用有用的信息 [3]。安全和 IT 是为了防止在安全措施上进行危险操作,防止发现漏洞,这些漏洞已经是智能电网机器的一部分,因此连接的物理设备与 EV 上认证的网络之间的不匹配。这种情况需要加强,以涵盖智能电网接入基础设施,因为电动汽车充电站技术 EV、EVSE 和智能手机应用是智能电网风险的方法。因此,如果攻击者从 EV 或 EVSE、驱动程序使用某些功能的智能手机应用程序发起攻击,则电网的物理安全可能是最大的风险 [4]。 A 一般。感兴趣的用户、智能电网和无线控制应用的双向交互技术,对安全意图的忽视成为电动汽车充电站故障控制技术的复杂潮流。图 (1)通信技术传输的智能电网下的电动汽车充电站技术。物理篡改、恶意软件上传和负载更改是对 EV 或 EVSE 智能手机的可能攻击 [5]。虽然是智能电网中最脆弱的部分,但恶意软件攻击者加载到 EVSE 可能会破坏 EV,当 EV 行驶和充电时,蠕虫可以很容易地在城市及其互连中从一个人传播到另一个人,因为它的电池来自路上还有其他几个 EVSE。

本文的综合结构如下:电动汽车在第二节中描述。充电站系统的组成部分。

在第三节.smartgrid 安全。在第四节中查看了黑客崩溃问题。在第五节。
Charaing station vs vulnerabilites 。在第六节威胁和

http://dx.doi.org/10.17758/EAP.EAP816010

充电站仪表内部的漏洞。在第 VII 节中。
充电桩攻击和攻击类型。最后在第八节得出结论。

图1 电动汽车充电站技术（10）

二、充电站系统组件

电动汽车的充电基础设施通常由无线电力服务和安全信息组成。充电站中的组件是LCD、电路板、无线网络通信（WIFI点、手机网络、蓝牙、智能电网、充电线协议）。如果没有安全技术,充电站就像街道上的电线杆,它们通过互联网进行通信以提供安全信息,并使用协议与充电站网络进行敏感通信,数据更新通过各种方式在充电站上传输网络协议。然而,驱动程序可能需要激励计划来利用计费价格的安全性,对数据计费加载的控制会遭受各种安全威胁。因此,减少充电中断是基于智能电网组件和电动汽车充电网络访问状态:物理访问是进入存在漏洞的无线设备,因为攻击者可以寻找不安全的通信。承载数据和通信的收费卡标识很容易伪造收费组件上的信息标识配置是不可能的:这不是一种完美的安全方式。连接到笔记本电脑到以太网的组件并设置 Web 浏览器或拒绝服务。此外。充电桩不安全通常是智能电网的实际隐患。

2-应用程序访问充电站,例如 EVSE 是可以用来收集数据的支付系统,它也是结合支付和数据收集通信,例如移动应用程序,EVSE 增加发票容量（以及许多其他)将需要网络通信,以由于 RS485,请务必确认 EVSE 是否需要以太网（Cat5 或 Cat6)或单元网格访问和调度,这样就不存在组件中小工具之间常用的这种通道的不安全性。实际上,让我们看看站是否有能力或参与确保您从未导航到

,

繁忙的车站开始。充电开始和充电停止一键通知,通过您的充电情况获得实时更新,检查充电状态的里程必须基于电动汽车类别。能源会话的成本取决于您已插入充电点、房屋时间表、电动汽车的轨道使用情况。从整个充电网络查看地图并前往数千个充电位置。卫星可以显示充电站到停车位;
Navigator 将找到您的方向,因此您需要获取信息和详细信息,例如实时、定价计费、充电位置的控制输出。

.

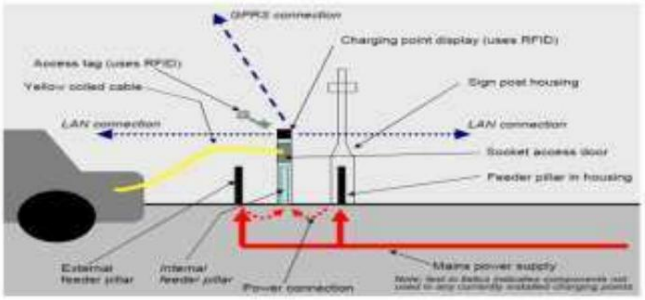

图 2. 充电点组成 (12)

三、智能电网安全

有关客户个人和位置信息的未加密信息的数据传输威胁到客户的隐私[14],例如中间人攻击可以更改信息以控制价格计费信息。智能电网由传感器、监视器、应用设备以及数据收集和分析组成的网络。所有这些都容易受到实时网络攻击。在与智能电网进行信息通信时,大多数可用的解决方案都忽略了数据传输的安全性。需要付出更多努力来确保电动汽车管理系统各个实体之间的安全、可靠的数据传输。智能电网和车队管理系统交换大量信息,例如充电站负载、电动汽车电池状态、交通信息和意外信息。智能电网、电动汽车和充电站中的事件和事故。任何安全攻击都可能影响智能电网、充电站和电动汽车的 ISO 运行。例如,电压或电流水平信息的虚假信息和更改可能会烧毁电动汽车和充电站中的电子元件。同样地。

四。黑客崩溃问题

公用设施需要安全信息来进行计费、需求响应和负载预测。然而,同样的信息可以揭示一个人的生活方式。每个电器都有一个独特的用电量签名,可以从整体使用模式中提取,指示用户在做什么,即在计算机上工作,犯罪分子可以利用此信息用于不同目的。营销公司可以在非竞争性定价期间使用此信息进行有针对性的营销或介绍。 E- 犯罪分子可以使用这些信息来确定日常生活或家庭,即何时

http://dx.doi.org/10.17758/EAP.EAP816010

房子里没有人,或者当有人独自在家中犯下入室盗窃或其他罪行时。通过篡改电表或在破解加密密钥 [9] 后更改信息来更改电表读数,可能会发生电力盗窃。除了专门的攻击和第三方入侵之外,智能电网还面临多种威胁[9-14],包括通过数据盗窃、电力盗窃、服务中断、设备物理损坏、拒绝他们的行为和市场欺诈。侵入智能电表、窃听无线通信或从公用事业的服务器窃取数据可以提供用户消费的细粒度计量信息 [9]。对充电站的网络攻击已经确定了与智能电网相关的计算机化安全系统面临的五个主要挑战[7] 包括大量敏感的信息客户、分布式控制设备、缺乏物理保护、薄弱的行业标准和庞大的依赖于网格的受感染利益相关者的数量。与其他典型系统一样,智能电网安全的关注点是机密性、完整性和可用性。机密性需要保护消费者和运营数据;消费者层面的计量和计费以及运营层面也需要完整性,以确保电网的稳定性;可用性意味着无论系统的状态如何,客户都可以继续传输和接收电力。智能电网面临与任何复杂计算机网络相同的安全挑战,需要外围防御和网络可见性。黑客的根本问题是,鉴于整个网络的庞大规模和互连性,蠕虫和病毒可以迅速传播。此外,鉴于网络的分布式特性,存在大量易受攻击的目标,例如管理密码通常位于之前且从未更改过原始设置。网络有几个入口点。此外,SCADA 系统的设计安全性不足;例如,西门子仍然使用硬编码密码来允许访问控制系统 [8],一旦受到破坏,可能会导致大规模的安全漏洞。

表一:漏洞充电站

1 客户安全		智能电表收集大量数据并将其传输给公司、消费者和支持信息
2 更大	智能设备数量	智能电网非常具有多智能组件,需要可管理的电力和网络需求 A 而且智能电网网络估计是互联网网络的 100 到 1000 倍。
3 物理安全		与传统电力不同,智能电网组件很容易不安全,因为设备有限,因此增加了物理访问的脆弱性
4直流电力系统的寿命		由于电力系统与寿命相对较短的 IT 系统共存,因此不可避免的过时设备仍在使用中。该设备可能充当弱安全点,并且很可能与当前的电力系统设备不兼容。
5传统之间的隐性信任	电力设备	虚假发送状态被认为容易受到数据欺骗。所以一个设备会影响另一个设备或不受欢迎的设备通信
6不同	团队背景	漏洞来自糟糕的团队之间的低效沟通
7使用	互联网协议	攻击者 - 基于协议的 IP 欺骗、IP Tear Drop 和拒绝服务 IP。使用IP的好处是提供了组件之间的团结,但是,如果IP被攻击了,那就是损坏

包括通过受感染设备的渗透、基于网络的入侵、受损的供应链和恶意内部人员。

五、充电站与漏洞

EV 的网络诊断更加复杂,容易受到不同类型的攻击。智能电网网络引入了传统电力的增强和改进功能。这些攻击者可能会在 EVSE 网络上将漏洞错误地传输到接入充电站。

六、充电站仪表内部的威胁和漏洞

没有单一的设备或机制可以提供充电站或充电点网络安全所需的所有必要安全措施。用于提高直流电网的性能并改变用电者的生活 由于电表是智能电网基础设施中的关键部件,智能电表可以容纳最有价值的数据（例如抄表和检查）。例如,需要抄表来支持许多智能电网应用和服务,包括自动抄表、计费、动态定价以及检测即将发生的停电和能源盗窃,这可以为公用事业和能源消费者带来极大的便利。然而,从智能电表收集的海量数据应该得到小心保护

http://dx.doi.org/10.17758/EAP.EAP816010

反对滥用。希望将安全机制纳入智能电表基础设施的设计和实施中,以提高系统的稳健性和弹性并获得能源消费者的信任。Skopik 等人。 [12] 分析了智能电表基础设施中的安全威胁和漏洞,详细分为三个层次:智能电表、公用事业和 Web 应用程序。第一层智能电表漏洞被归类为对智能电网的攻击。 ID客户、EV的位置、运行时间和数据、EV的牌照是影响下一个充电站的因素。深意来说,如果其中一个被攻击,都考虑损坏计算但是,抄表是不确定的,以正确用电。

这些还可能包括查询、警报或通知。
影响系统稳定性和可靠性以及安全性 配置数据 配置数据（系统操作设置和安全凭证,还有警报阈值、任务计划、策略、分组信息等)会影响组件的行为,并可能影响更新的电力系统稳定和安全时间,时钟设置时间用于发送给其他实体的记录。相位或测量与控制系统动作直接相关。此外,优化使用关税信息也需要时间。它还可以用于某些安全协议中确定通信对等方是否有权发送和接收命令和数据。此类策略可能包括效果系统控制系统稳定性、可靠性及其凭据和角色的列表。汽车制造商, 他们的正确性是关键市场的能源系统供应商可能会告知消费者新的或临时的税收作为通过竞争最终决定客户隐私的基础。

七。充电桩攻击和攻击类型_

充电桩 攻击记忆漏洞可能由具有不同想法的攻击者操作,可能对网络造成不同程度的破坏。攻击者不区分员工和客户的不同动机。因此作者尝试了攻击者的分类群,如 1. 非恶意攻击者,他们告诉我们安全操作系统令人困惑和困惑,那些有强烈的破坏 IOP 的愿望但好奇心是智力挑战 2. 报复是驱使消费者对他人进行报复关闭权力,不可能弄清楚他们的问题。

3. 在当今更明显的事件中,指定智能电网的恐怖分子是影响数百万人的有吸引力的目标 4. 说明消费者的财务目的相互攻击[5],[6],对各种各样的攻击进行分类 Component –wise 是远程终端单元 (RTU) 目标,它对解决智能电网设备故障的工程师感兴趣,因此,恶意用户将问题归咎于导致关闭的问题,protocol-wise 是协议攻击者本身,其作为逆转决定被谋杀可被假日期感染。拓扑方面具有强大的功能,包括拒绝服务攻击,使电源运行保持充满电。

这些是更危险的攻击者,如 [7]、[10]。

1. 恶意软件传播,即感染智能电表和无线服务,是自杀式攻击者,替换某些功能或添加虚假日期 2. 数据库链接期间的访问:控制系统仍然存在数据库并记录自己的活动,但是对于熟练的攻击者的访问可能会利用系统网络上的弱数据库管理。

3. 通信设备受损:多路复用器将工作直接危险的通信设备视为预测未来威胁的后门。 4. 虚假信息注入:注入虚假价格、虚假电表数据会对电力市场造成巨大的财务影响。 [19] 5.网络容量:漏洞被尝试使用IP协议和TCP/IP成为更容易攻击的目标,使DOS攻击可以破坏信息承载,以延迟找出智能电网问题。

6.窃听和流量分析 网络流量的导师一直是敏感的传输,包括计费信息、无线基础设施和攻击者的好奇心。

7. Modbus 安全问题:Modbus 协议是 SCADA 系统的一部分 SCADA 一词是指跟踪监视器的计算机系统和协议 [18]

并控制工业、基础设施或基于设施的过程,例如智能电网过程。它负责交换控制工业过程所需的 SCADA 信息。鉴于 Modbus 协议不是为高度安全的关键环境而设计的,因此可能存在多种攻击,包括:(a) 向从设备发送虚假广播消息（广播消息欺骗）,(b) 将真实记录的消息重播回主设备（基线响应回放）,（c）锁定主机并控制一个或多个现场设备（直接从机控制）,（d)向所有可能的地址发送良性消息以收集设备信息（Modbus网络扫描）,（e)读取Modbus消息（被动侦察）,（f)延迟发送给主机的响应消息（响应延迟）,以及（g）使用适当的适配器攻击计算机（Rouge interloper)[19]。

八。结论

充电站技术使其很容易成为攻击者的目标。特别是,级联攻击和蠕虫感染可以比其他组件传播得更快。本文详细介绍了相关示范项目的研究情况和研究成果,电动汽车设备和技术是承载高安全风险的负载之一。网络安全是一个日益受到关注的问题,对于成功部署智能电网系统非常重要和关键 智能电网的庞大性和增强的通信能力使其更容易受到网络攻击。智能电网条件下的电动汽车充电站系统探讨了电动汽车充电站的关键技术并指出了网络攻击。

充电站是关键部件之一

http://dx.doi.org/10.17758/EAP.EAP816010

发展电动汽车充电站。电动汽车充电站技术可以促进智能电网安全,符合当前节能的能源利用模式。因为智能电网由于拥有大量攻击者而容易受到攻击,攻击者可能会危及负载、智能电表、输配电设备、PMU、传感器、计算机等。我们回顾了智能电网充电站的网络攻击者问题。由于智能电网技术被视为一项关键基础设施,承担充电站项目的企业需要与智能电网系统密切合作。应识别所有漏洞并找出智能电网的足够解决方案。

参考

[1] Arman, NA, Logenthiran, T., & Woo, WL (2015)。微电网分布式储能系统的智能能源管理。2015 年IEEE 创新智能电网技术 - 亚洲 (ISGT ASIA)。 doi:10.1109/isgt-asia.2015.7387076 http://dx.doi.org/10.1109/ISGT-Asia.2015.7387076 [2] Bhagyashree Patil 和 Maruti Limkar。 （2015 年）。基于机器对机器通信的智能计量系统。伊杰特,V4(06)。 doi:10.17577/ijertv4is060396 http://dx.doi.org/10.17577/IJERTV4IS060396 [3] Bhatti, AR, Salam, Z., Aziz, MJ, Yee, KP, & Ashique, RH

（2016 年）。使用光伏充电的电动汽车:现状和技术回顾。可再生能源和可持续能源评论,54, 34-47。 doi:10.1016/j.rser.2015.09.091 http://dx.doi.org/10.1016/j.rser.2015.09.091 [4] Collins, L. (2014)。保护基础设施。网络安全和 IT基础设施保护,247-267。 doi:10.1016/b978-0-12-416681-3.00010-0 http://dx.doi.org/10.1016/B978-0-12-416681-3.00010-0 [5] 客户、充电站之间的通信减少交互协议和充电站管理系统。

（2014）。第三届智能电网和绿色 IT 系统国际会议论文集。 doi:10.5220/0004971801180125 http://dx.doi.org/10.5220/0004971801180125 [6] Deng, B., & Wang, Z. (2011)。基于智能电网的电动汽车充电站技术研究。 2011亚太电力与能源工程会议。 doi:10.1109/appeec.2011.5748759 http://dx.doi.org/10.1109/APPEEC.2011.5748759 [7] Elliman, R., Gould, C., & Al-Tai, M. (2015)。回顾当前和未来的电能存储设备。 2015 年第 50 届国际工程 (UPEC)。 doi:10.1109/upec.2015.7339795 http://dx.doi.org/10.1109/UPEC.2015.7339795

大学 力量 会议

[8] 交通工程国际会议（5th : 2015 : 中国大连）。 (2015).ICTE 2015:第五届交通工程国际会议论文集:2015 年 9 月 26-27 日,中国大连。

[9] 立维腾 Evr-Green 电动汽车充电站。 (nd)。已取回从 http://www.leviton.com/OA_HTML/SectionDisplay.jsp?section=37818&minisite=10251

[10] Li, H., Sun, GM, & Chu, Y. (2012)。基于Weblogic的电动汽车充电站综合监控系统设计。 AMM, 241-244, 2004-2009。 doi:10.4028/www.scientific.net/amm.241-244.2004 http://dx.doi.org/10.4028/www.scientific.net/AMM.241-244.2004 [11] Marcincin, O., & Medvec, Z （2015 年）。电动汽车的有源充电站。 2015第16届国际电力工程科学会议（EPE）。 doi:10.1109/epe.2015.7161084 http://dx.doi.org/10.1109/EPE.2015.7161084 [12] Mousavian, S., Erol-Kantarci, M., & Ortmeyer, T. (2015)。弹性电动汽车基础设施的网络攻击保护。2015 IEEE Globecom 研讨会 Wkshps）。 doi:10.1109/glocomw.2015.7414174 http://dx.doi.org/10.1109/GLOCOMW.2015.7414174

（GC

[13] Nie, X., Liu, J., Xuan, L., Liang, H., Pu, S., Wang, Q., & Zhou, N. （2013）。电动汽车充电站在线监测与综合分析系统。 2013 IEEE PES 亚太电力与能源工程会议 (APPEEC)。 doi:10.1109/appeec.2013.6837206 http://dx.doi.org/10.1109/APPEEC.2013.6837206 [14] Singh, M., Kumar, P., & Kar, I. (2012)。一种兼容车辆到电网场景的电动汽车充电站模型。 2012 年 IEEE国际电气会议。 doi:10.1109/ievc.2012.6183223

车辆

http://dx.doi.org/10.1109/IEVC.2012.6183223 [15] Ma, C., Rautiainen, J., Dahlhaus, D., Lakshman, A., Toebermann, JC, & Braun, M. (2015) .电动汽车在线优化充电策略。Energy Procedia, 73, 173-181。

http://dx.doi.org/10.1016/j.egypro.2015.07.667 [16] Falk, R. 和 Fries, S. (2012)。电动汽车充电基础设施安全考虑和方法。过程。互联网,58-64。

[17] http://www.chargepoint.com/访问 25-07-2016

[18] Yuvaraj S. Patil Dr. Swati V. Sankpal 夫人,5 月 15 日第 3 卷第 5 期， “智能电网网络安全调查”,国际计算与通信近期和创新趋势期刊 (IJRITCC)， ISSN:2321-8169,PP:2503 - 2507， DOI:10.17762/ijritcc2321-8169.150502

[19] Aloul, F., Al-Ali, AR, Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. （2012）。智能电网安全:威胁、漏洞和解决方案。国际智能电网和清洁能源杂志， 1-6。 doi:10.12720/sgce.1.1.1-6 http://dx.doi.org/10.12720/sgce.1.1.1-6

S.AHMED 收到 这 多发性硬化症 2008 年获得马来西亚 UUM 大学 (UUM) 计算机科学学位。他目前是助理讲师。主要研究方向为可再生能源、电动汽车、信息通信技术。

FM Dow 获得了萨尔特大学电气工程系的学士学位，

2003 年获得利比亚,2013 年获得利比亚学术电气工程硕士学位。他目前在利比亚研究、科学和技术管理局工作。他的研究兴趣包括智能电网和可再生能源。

.