



对等网络与能源互联网安全

任建伟¹, 安春燕², 刘昀¹, 李坚³

(1. 国网冀北电力有限公司信息通信分公司, 北京 100053;

2. 全球能源互联网研究院, 北京 102209;

3. 国网冀北电力有限公司, 北京 100053)

摘要: 对等网络技术在互联网中得到了广泛的应用, 它具有的自愈、自组织等特性可以满足能源互联网在高可靠性、节点即插即用等方面的需求, 但对等网络也带来了新的安全威胁。研究了对等网络的抽象特征, 分析了在能源互联网中应用对等技术将面临的主要安全威胁, 并给出了相应的安全建议。

关键词: 能源互联网; 对等网络; 安全

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2015387

Security on peer to peer networking in energy internet

REN Jianwei¹, AN Chunyan², LIU Yun¹, LI Jian³

1. State Grid Jibei Information and Communication Company, Beijing 100053, China

2. Global Energy Interconnection Research Institute, Beijing 102209, China

3. State Grid Jibei Electric Power Company, Beijing 100053, China

Abstract: Peer to peer systems are widely deployed in the internet. Its self-healing and self-organizing framework will facilitate plug and play, high reliability and other features of the energy internet. But it brings new threat. The abstract features were researched. The threats introduced by peer to peer networking in the energy internet scenario were analyzed, and accordingly countermeasures were given.

Key words: energy internet, P2P network, security

1 引言

能源互联网是以新能源和信息技术深度结合为特征的能源体系^[1], 并具有以下主要特征^[1-3]:

- 支持能量流和信息流耦合, 支持能量和信息的双向流动, 其中能量流包括电能、天然气、热能、风能、太阳能等多种能态的可再生新能源;

- 支持即插即用方式的分布式能量源和负载接入;
- 支持自愈, 具有高可靠性。

学术界和工业界对能源互联网网络架构展开了积极的探讨, 认为能源互联网的构建应采用互联网思维、基于智能电网实践^[4], 其骨干网以特高压电网为基础, 而能源局域网则以微网和分布式能源等能量自治单元作为主要组成部分^[4], 采用集中和分布相结合、层级结构和对等 (peer to

收稿日期: 2015-12-01; 修回日期: 2015-12-11

基金项目: 国家电网公司科技项目“能源互联网信息通信体系架构研究”(No. SGRIXTKJ[2015]253)

Foundation Item: Science and Technology Project of State Grid Corporation of China “Research on the Architecture of Information Communication System for Internet of Energy”(No. SGRIXTKJ[2015]253)

peer,P2P)结构相结合的自组织网络架构^[5]。

因此,对等、自组织的网络将是能源互联网整体架构的重要组成部分。对等架构在互联网发展中具有重要的作用,对等网络承载了内容分发和共享、实时视、音频通信等诸多业务,但目前对能源互联网架构的讨论主要针对分层架构和云计算、SDN 等集中架构,缺少对对等架构的探讨。

对等架构支持分布式部署、即插即用、自愈能力强,这些都是能源互联网必备的主要特征,但安全性是对等架构面临的主要挑战。本文基于能源互联网业务需求,对对等网络架构的功能和特征进行了抽象,分析了与这些特征关联的主要安全威胁,从而为对等网络技术应用于能源互联网提出原则性的安全建议。

2 P2P 技术及其在电网中的应用

P2P 技术指业务系统或网络中的节点从功能上是对等的。它首先作为一种 Internet 的计算模式被提出,与传统互联网业务的客户机/服务器(C/S)模式不同,P2P 模式强调节点既是资源的提供者也是资源的使用者。业务模式层面的对等技术在能源互联网中已有探讨^[6],能源互联网应在用户之间、供应商之间支持对等模式的能源交易^[7],用户将具备能源消费、能源生产双重身份,通过智能电表连接的用户终端设备可同时作为能源互联网的终端和服务节点,如一个家庭在消耗电能的同时,其太阳能电池板可以作为微型发电机向电网输送富余电能,家庭的电动汽车也可作为电网的储能节点。

从网络技术的角度理解,P2P 泛指由对等节点构成的各种网络结构。P2P 作为重叠的逻辑网络构建在物理网络上,如图 1 所示,P2P 重叠网与底层物理网具有独立的地址和标识空间、拓扑结构、路由协议、数据转发和节点管理等机制,重叠网的对等节点通过虚拟链路连接,一条虚拟链路为物理网络中一条经过多跳转发的通路。

P2P 网络具有分布式、自组织、自配置和自愈等特性,从而具有更好的可扩展性、更强的顽健性和更低的构建和管理成本,因此人们已尝试将其思想应用于智能电网中,如将分布式的量测数据管理系统(MDMS)节点部署于智能电表附近,构成对等网络^[8],从而减小数据收集和处理时

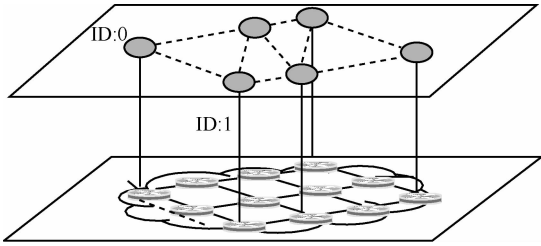


图 1 P2P 重叠网络和底层物理网络

延,提高电网的实时调控能力,减少通信带宽;以智能电表构成的多跳网状网作为高级量测体系(advanced metering infrastructure,AMI)的局域网架构,由智能电表完成计量数据的路由和转发^[9],将 P2P 重叠网络的自组织特性与底层的短距无线网络很好地结合,无需部署额外的基础设施就可由智能电表完成较大物理区域的数据路由和转发。

3 安全威胁分析

对等网络虽有上述诸多优点,但带来这些优点的对等、自组织等技术本质也使网络不可避免地面临新的安全威胁^[9]。虽然,P2P 网络具有不同的拓扑结构、节点管理机制、寻址和路由机制^[10],而且能源互联网中对等技术应用的具体方式也未知,但仍可抽象出对等网络的共性特征,基于这些特征来分析在能源互联网中采用对等网络技术可能面临的安全威胁。

3.1 应用层安全

P2P 业务的核心应用是内容(或数据)共享,能量互联网业务应用则包括能量和信息流两种形态,信息流应用的业务本质与互联网中一致,因此这里重点讨论能量流相关的应用层。由表 1 可知,传统互联网和能源互联网中的对等业务都可抽象为(资源 ID,资源描述),因此能量互联网与传统互联网 P2P 业务具有相同的抽象模型,即用户发布可共享的资源 ID 及相关资源描述,通过应用层路由功能搜索存储有特定资源 ID 的节点,其中,资源 ID 常为资源描述的散列值,它唯一标识了符合特定资源描述的资源。

根据应用层业务抽象描述和应用层路由功能的一致性,基于传统互联网 P2P 业务的安全威胁研究成果,可以有效地分析能源互联网对等业务可能面临的安全威胁以及相应的安全对策,见表 2。

表 1 传统互联网和能源互联网对等业务对比

业务	对等业务请求实例	抽象描述	对等网络应用层路由
内容共享	用户 A 需要名为 x 的一部电影	(内容 ID,内容描述)	搜索可提供此内容的用户
能量微网	在某小区的用户 A 需要持续几小时的 y 度电能	(能量 ID,能量描述)	搜索可提供此能源的用户



表 2 对等业务安全威胁及对策

安全威胁	威胁描述	能源互联网所需安全对策
隐私泄露	通过用户共享的资源和服务,泄露了用户的隐私信息	隐藏能源提供者的身份信息
rational attack ^[11]	用户总是理智的,希望利益最大化,从而只愿意下载资源而不提供资源	合理的业务模式对能源消费和供给的精确计价
洪泛攻击	洪泛业务请求,消耗对等网络中节点的运算能力和带宽	基于业务行为的应用层攻击检测
内容污染 ^[12]	用户提供的资源内容与描述不一致,如提供的能源质量或时长低于描述,从而变相盗取能源互联网资源	能源的精确计量

3.2 路由相关的安全威胁

对等网络根据路由机制的不同分为无结构和有结构,前者采用洪泛的方式进行路由,从安全性和可扩展性角度考虑都不适合能源互联网。结构化的对等网络则根据一定的标识空间划分提高了路由效率,分布式散列表(distributed hash table, DHT)^[10]由于其优越的可扩展性成为结构化对等网络主要的路由技术。

DHT的基本功能是完成(key, value)对的搜索, key 为要搜索的资源,如第 3.1 节中所述的能源 ID, value 则是存储这个 key 相关信息的节点地址。根据网络的不同性能要求设计了不同的 DHT 结构, $O(1)$ DHT 和单跳 DHT 用更大的路由表换取了常数跳甚至单跳的数据搜索和路由性能,各种多跳 DHT 则对标识空间进行了结构划分,通过多跳完成路由,有较小的路由表,但其路由跳数通常为 $O(\lg N)$ (N 为网络中的总节点数)。

对于能源互联网,以下对等网络中路由相关的攻击是需要主要考虑的。

(1) Churn 攻击

和所有的路由机制一样,当对等网络有拓扑更新时,需要与其他节点的交互来学习路由表、发布路由信息,使全网节点得以更新路由表。因此,恶意节点可以利用对等网络的自组织特性频繁地加入和退出网络,激发大量的路由更新信息,使网络处于不稳定状态,此即 Churn 攻击。

能源互联网中,节点具有即插即用特性,能源互联网的远端节点相比传统互联网终端更易出现硬件连接的不稳定,这些特性都将加剧 Churn 攻击的影响。此外,在能源互联网中,Churn 攻击的后果也将远大于传统互联网,以电网为例,部分负载和发电机组的不稳定都将对电网调控带来巨大压力,最终可能导致整个电网发生故障。在构建能源互联网中的对等网络时,以下对策可减少 Churn 攻击的影响:

- 采用分层结构的对等网络,或只在能源互联网的边

缘构建对等网络,通过限定对等网络路由扩散区域,限定 Churn 攻击影响范围;

- 将生命周期长的节点(如智能电表)加入对等网络中,而动态性较强的节点(如用户用电终端)则只通过长生命周期的节点加入,不参加对等网络的路由;
- 部署行为检测功能,有效检测 Churn 攻击;
- 实施更严格的节点接入控制。

(2) 不正确的路由更新

在进行路由更新时,恶意节点可以发送无效或恶意的路由更新信息,使正常节点的路由表中毒从而达到多种攻击目的,如使路由表中恶意节点占更大的比例,从而控制网络路由,扩大窃听等其他攻击的成效;将路由指向不正确或不存在的节点,由于对等网络路由的自愈能力,最终路由仍有很大的概率到达正确节点,但此攻击增加了路由查找跳数,造成网络性能下降甚至引起网络拥塞;通过路由反射实施分布式拒绝服务 DDoS 攻击,将路由指向特定的被攻击对象;进行路由劫持,劫持部分对等网络,这种攻击也被称为 eclipse 攻击,它使被攻击节点或网络的一部分只与选定的逻辑节点(通常是恶意节点)进行连接,从而可进行中间人攻击或拒绝服务攻击。

根据以上对等网络路由攻击的原理,能源互联网中应对对等网络路由攻击的对策如下:

- 采用分层网络结构,只允许生命周期较长或信誉较高的节点(如归属于能源提供商的设备)参加对等网络路由,相对稳定的拓扑使恶意节点通过不正确的路由更新信息进行攻击的难度增大;
- 在节点上部署路由异常检测,并对正确路由进行确认,通常可规避绝大多数不正确的路由信息;
- 要求路由信息发送者对路由更新信息进行签名。

(3) 身份窃取攻击

当路由查找信息到达恶意节点时,恶意节点可以宣称它就是负责这个 key 的目的节点,从而劫持路由和数据查找请求,更进一步的,攻击者可以伪造和破坏数据,如攻击

者可以宣称它负责存储特定用户的智能电表计量数据,从而提供虚假的计量数值;或攻击者可宣称对某一能源 ID 负责,从而恶意提供与能源描述不符的能源。设计路由算法使其可检测 ID 与拓扑的一致性、要求节点提供 ID 证明都有助于应对身份窃取攻击。

以上各种攻击还可以组合成复杂的攻击链,如 Sybil→incorrect routing update→eclipse→identity theft/DoS/DDoS,通过 Sybil 攻击使一个物理节点控制多个逻辑节点,放大后续路由攻击的效果,然后通过不正确的路由更新实施 eclipse 攻击,最终使恶意节点能够完成身份窃取或实施拒绝服务攻击。

值得指出的是,利用能源互联网更强的可管控能力,有控制地利用以上路由攻击手法也可以得到正面的效果。如利用少量的 Churn 可以复位全网的路由表,从而帮助破坏其他路由攻击的效果;有意地加入少量的不正确路由可以使数据随机地转发到迂回路径上,从而破坏窃听、密码分析等攻击。此外,在企业或家庭用户小区的能源局域网中,对无线网络基础设施进行信号截获是很难防御的攻击,由于对等网络路由的特性,攻击者无法将从无线链路截获的信息与特定的用户对应起来,从而可有效提供用户隐私保护,加大密码分析的难度,提高机密性和完整性。

3.3 标识分配和管理相关的安全威胁

网络标识分配和管理是组网的关键,为了保证对等网络去中心化、动态自组织等特性,P2P 组网技术趋向于无中心的标识分配,在节点加入网络时由节点的底层物理网络标识(如 IP 地址)等参量计算其在对等网络中的标识。由于物理网络存在地址欺骗等安全威胁,对等网络中相应地出现了新的标识相关的安全威胁。表 3 总结了各种异构的对等网络标识管理的共性特征,分析了各种特征可能导致的安全威胁,并给出了相应的建议。

标识分配是节点加入对等网络的第一步,标识相关的攻击经常与其他攻击手法结合,如攻击者通过 Sybil 攻击得到多个标识从而伪造网络中的多个逻辑节点,提高窃听、路由破坏等攻击的成功率。在能源互联网中,攻击最终体现为恶意节点有更大的概率被选为能源提供节点,从而增加获利;更多的业务通过恶意节点进行路由,攻击者可通过信息收集得到能源互联网用户的隐私信息,并增加密码分析的成功率。

4 结束语

对等网络经过十多年的发展,在互联网中已占据了重要的地位,承载了大量互联网业务。在能源互联网中,对等能源交易将是能源互联网的特色业务,采用对等技术的能源微网也将是能源互联网的重要组成部分。本文从应用层业务、标识管理、路由机制 3 个方面对对等网络的特征进行了抽象,分析了能源互联网中应用对等架构可能存在的安全威胁,并提出了相应建议。

参考文献:

[1] RIFKIN J. The third industrial revolution: how lateral power is transforming energy, the economy and the world [M]. Berlin: Macmillan, 2011: 27-68.

[2] 田世明, 栾文鹏, 张东霞, 等. 能源互联网技术形态与关键技术[J]. 中国电机工程学报, 2015, 35(14): 3482-3494.

TIAN S M, LUAN W P, ZHANG D X, et al. Technical forms and key technologies on energy internet [J]. Proceedings of the CSEE, 2015, 35(14): 3482-3494.

[3] 刘振亚. 全球能源互联网[M]. 北京: 中国电力出版社, 2015.

LIU Z Y. Global energy interconnection [M]. Beijing: China Electric Power Press, 2015.

[4] 杨新法, 苏剑, 吕志鹏, 等. 微电网技术综述 [J]. 中国电机工程学报, 2014, 34(1): 57-70.

表 3 ID 分配和管理相关的主要安全威胁

对等网络标识特性	主要安全威胁	能源互联网可行对策
标识唯一性, 逻辑标识与物理标识间的独立性	Sybil 攻击: 一个物理节点得到多个逻辑 ID, 假冒对等网络中的多个逻辑节点, 从而扩大恶意节点在业务和路由中的优势	增加标识这一资源的使用代价, 使逻辑标识与唯一可信的物理标识对应; 由逻辑上集中(物理上仍可分布部署)的功能节点完成标识分配和管理
采用分布式散列表路由机制的对等网中, 标识决定了逻辑节点负责某一特定信息空间的内容存储、路由以及节点在路由中的位置	ID mapping 攻击: 节点通过伪造身份有选择性地获取特定的标识, 使自己在数据路由中处于关键位置	采用结构化的标识, 至少保证标识的一部分无法由用户控制
节点通过协议与其他节点交互信息以完成自组织的节点加入(bootstrap), 得到下一跳路由等关键信息	窃听、截获, 信息收集	设计节点间协议交互的机密性和完整性保护机制



- YANG X F, SU J, LV Z P, et al. Overview on micro-grid technology[J]. Proceedings of the CSEE, 2014, 34(1): 57-70.
- [5] 赵海, 蔡巍, 王进法, 等. 能源互联网架构设计与拓扑模型[J]. 电工技术学报, 2015, 30(11).
- ZHAO H, CAI W, WANG J F, et al. An architecture design and topological model of inter grid [J]. Transactions of China Electrotechnical Society, 2015, 30(11).
- [6] ZHOU J, HU R Q, QIAN Y. Scalable distributed communication architectures to support advanced metering infrastructure in smart grid [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(9): 1632-1642.
- [7] WANG A, ROGERS J. Peer to peer electricity: beyond the smart grid[M]. [S.l.]: AXL Incorporated, 2012.
- [8] CAI F, FARANTATOS E, HUANG R, et al. Self-powered smart meter with synchronized data[C]//2012 IEEE Radio and Wireless Symposium (RWS), January 15-18, 2012, Santa Clara, CA, USA. New Jersey: IEEE Press, 2012: 395-398.
- [9] YUE X, QIU X, JI Y, et al. P2P attack taxonomy and relationship analysis [C]//The 11th International Conference on ICAC, February 15-18, 2009, Phoenix Park, Korea. New Jersey: IEEE Press, 2009: 1207-1210.
- [10] 张春红, 裘晓峰, 弭伟, 等. P2P 技术全面解析 [M]. 北京: 人民邮电出版社, 2010.
- ZHANG C H, QIU X F, MI W, et al. Comprehensive analysis of P2P technology[M]. Beijing: Posts and Telecom Press, 2010.
- [11] Khan: vulnerabilities of P2P systems and a critical look at their solutions [EB/OL]. [2006-11-01]. <http://medianet.kent.edu/techreports/TR2006-11-01-p2pvuln-EK.pdf>.
- [12] LIANG J, KUMAR R, XI Y, et al. Pollution in P2P file sharing systems[C]//24th Annual Joint Conference of the IEEE Computer and Communications Societies, March 13-17, 2005, Miami, Florida, USA. New Jersey: IEEE Press, 2005: 1174-1185.
- [13] DINGER J, HARTENSTEIN H. Defending the sybil attack in P2P networks: taxonomy, challenges, and a proposal for self-registration [C]//The 1st International Conference on Availability, Reliability and Security, April 20-22, 2006, Vienna, Austria. New Jersey: IEEE Press, 2006.
- [14] CERRI D, GHIONO A, PARABOSCHI S, et al. ID mapping attacks in P2P networks [C]//IEEE Global Telecommunications Conference, November 28-December 2, 2005, Saint Louis, USA. New Jersey: IEEE Press, 2005.
- [15] STUTZBACH D, REJAIE R. Understanding churn in peer-to-peer networks [C]//The 6th ACM SIGCOMM Conference on Internet Measurement, October 25-27, 2006, Rio De Janeiro, Brazil. New York: ACM Press, 2006: 189-202.
- [16] GANESH L, ZHAO B Y. Identity theft protection in structured overlays [C]//The 1st IEEE ICNP Workshop on Secure Network Protocols, November 6, 2005, Boston, Massachusetts, USA. New Jersey: IEEE Press, 2005: 49-54.
- [17] LI J, QIU X, JI Y, et al. Researches on secure proximity distance defending attack of finger table based on chord [C]//The 11th International Conference on Advanced Communication Technology, February 15-18, 2009, Phoenix Park, Korea. New Jersey: IEEE Press, 2009: 1923-1927.
- [18] PUTTASWAMY K, ZHENG H, ZHAO B. Securing structured overlays against identity attacks[J]. IEEE Transactions on Parallel and Distributed Systems, 2009, 20(10): 1487-1498.

[作者简介]



任建伟(1980-),男,国网冀北电力有限公司信息通信分公司高级工程师,主要从事电力通信安全研究与运维工作。



安春燕(1987-),女,博士,全球能源互联网研究院工程师,主要从事无线通信、电力线载波通信技术研究工作。



刘昀(1980-),女,博士,国网冀北电力有限公司信息通信分公司高级工程师,主要从事电力市场、信息通信安全等工作。



李坚(1987-),男,国网冀北电力有限公司工程师,主要从事电力信息安全研究与管理工作。