

面向配用电网的无线公网安全监测的研究

配用电智能设备和业务接入运营商网络后,数据通过运营商的无线网络、IP承载网传送到电力侧信息网络,电力公司无法控制、管理运营商的网络,数据传输的安全性难以得到保障。因此针对无线公网中面临的安全威胁,研究配电网公网无线接入安全技术方案,在配用电生产控制业务通信方法、配用电主站系统公网安全接入方法以及无线公网通道检测方面实现技术创新,提高配电通信网公网接入的安全水平。

刘燕龙 范群滔/广东电网有限责任公司梅州供电局
韦荣桃/华北电力大学电气与电子工程学院

0 引言

随着智能电网研究与实践的推进,传统意义上的电网正逐步与信息通信系统、监测控制系统相互融合,电力通信系统与电力系统融合得越来越密切,并且在电力系统中具有重要地位,电力通信网安全很大程度上影响着电网安全,所以电力通信网安全是电网安全的重要组成部分^[1]。网络安全在电力系统中的地位正在不断提高,针对电力领域的网络安全保护系统正在一步步变得更高效。目前电力信息网络采用安全分区、网络专用、横向隔离及纵向认证的安全防护体系。安全分区是指将生产控制分区的业务和信息管理分区的业务分别进行处理;网络专用是指为业务的统一协调分配建立专用的通信网络,使得控制数据能够在专用的网络中进行传输;横向隔离是针对电力行业设计的一种单向隔离设备,用来将生产控制分区的网络和信息管理分区的网络进行横向隔离;纵向认证是针对电力行业设计的一种纵向加密认证设备,用来对纵向传输的网络信息进行安

全加密,并支持一种安全认证机制^[2]。

配电网的业务主要是通过移动设备终端接入无线公网中,CDMA/3G/4G等无线公网接入技术在配电网中得到广泛应用,且接入数量将会持续快速增长。但是主要的通信路径是无线公网,社会的其他外部业务数据也是通过公网进行传输,且无线公网的网络传输协议也会有很多不足,这些都会导致信息传输网络的不安全性,如窃听、伪装、流量分析及拒绝服务等对网络产生不利的影响。伴随着互联网和计算机的快速发展,网络攻击方式也在不断更新变化,网络攻击的多样性和变异性对于通信网络的安全性产生了巨大威胁。来自内外部的安全风险给网络安全工作带来了极大的压力与挑战,因此,开展配电网公网无线接入安全技术研究与应用极为必要,通过配用电业务及智能设备接入方式、无线公网通道监测和安全防护等方面实现技术创新,提高配电通信网的安全性。

1 配用电通信网的安全需求

随着电力系统业务领域不断扩张,电网的服务范围也在不断扩大,相应的配用电规模也迅速改变,需要添加很多新的设备来满足配用电业务的发展需求,由这些设备组成的通信网络也面临着越来越大的挑战,现有的配用电网络无法应对新兴的各式各样的网络攻击,配用电通信网络的数据将面临很大的威胁,配用电通信网络的数据包括配用电网中的电表数据、用户平时的用电信息



刘燕龙/工程师

关键词/Keywords

配用电·
无线公网·
监测·

数据等，甚至有些数据具有很高的私密性，如果这些数据被盗取或丢失，将会导致配电通信网的通信遭到损害，同时会对用户带来很大的影响，以及很可能会有损害用户利益的风险，从而用户对电网的信心将会降低很多，所以需要一种更高效的方法来保护配用电通信网的数据去面对多变的网络威胁。首先，需要全面分析配用电通信网中存在的问题，找到导致这些安全问题的关键原因，从而为接下来的研究打好基础。

通过终端接入方式进入通信网的设备有开关站、环网柜、配电室、配电变压器、柱上开关、配电线路、分布式能源站点、电动汽车充电站和用电计量器等。这些设施将不断产生各种业务数据，需要被及时、准确且安全地传输至主站，以实现配电与用电业务采集的自动化^[3]。需要采用一种面向电力系统领域的单向横向隔离设备将电力系统网络的信息管理分区与生产控制区分开，这种设备是被国家机构认可的，并且被统一认证监测过的，它能够达到的隔离效果接近于物理隔离效果；系统设备需要具备能够防御火灾的保护机制，针对盗窃行为采取的保护措施，以及防止遭遇破坏的安全保护措施；系统的主站前置机需要采用加强型的安全防御操作系统，该操作系统是需要被国家机构许可、认证的，该操作系统对于任何形式的访问都有很严谨的操控机制来管理；由于前置机使用的信息传输网络是公用网络，所以需要把前置机放在安全接入分区中，并使用面向电力系统的正反向隔离设备将前置机与系统的通信区域分开；为了保证数据的安全性，需要使用一种审计机制来管理数据的传输^[4]。配用电通信网不同业务所面临的安全威胁如表1所示。

所以，面向配用电领域的不同业务信息需要整体的保护机制，并结合为综合业务安全保护方案，这个方案需要把配用电通信网中的所有业务安全问题考虑进去，并有系统性的保护机制，另外可以融入当前主流的前沿技术来提高方案的有效性和全面性，例如虚拟交换网络等。系统需要更高效、更安全的运行管理机制来保证系统的稳定性。

2 配用电主站系统的无线公网接入安全方案

配用电主站系统无线公网安全体系由数据安全、接入安全和业务安全三部分组成，如图1所示。

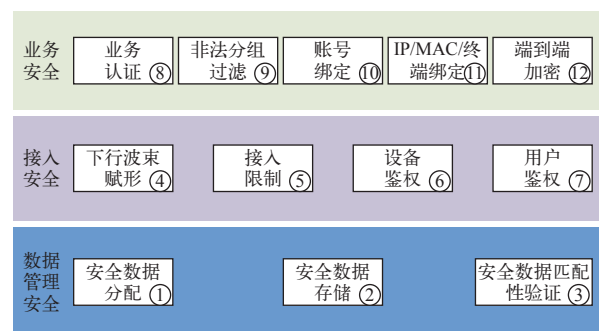


图1 配用电主站系统无线公网安全体系

无线通信业务数据直接接入公司信息内网时，主要采取数据加密、口令和指纹技术、终端加固及身份认证等终端安全措施，通道加密和数字证书等通道安全措施，以及部署信息内网安全接入平台等接入安全措施，保障业务数据的安全、可靠传输，如图2所示。

在一些具体应用中，业务数据只能先传送到公司的外部网络中，进入到外部网络后，这些业务数据下一步才能进入公司的内部网络。需要安

表1 配用电通信网不同业务所面临的安全威胁

项目	主要内容
网络接入安全	用户身份、行为踪迹、实体身份、地理位置、加密密钥分发、信令数据加密、用户信息和消息认证等无线链路网络的安全
核心网网络安全	实体间身份认证、消息认证、信息加密和欺骗信息采集等网络实体间的数据交互安全
用户安全	基站安全接入，包括用户安全加密认证、链路保护等
应用安全	用户和服务商的通信信息安全，各类实体之间身份认证、应用数据重放攻击检测、数据完整性保护和接收确认等
安全特性可见性与配置能力	用户获得安全性是否开启、服务是否需要安全服务等

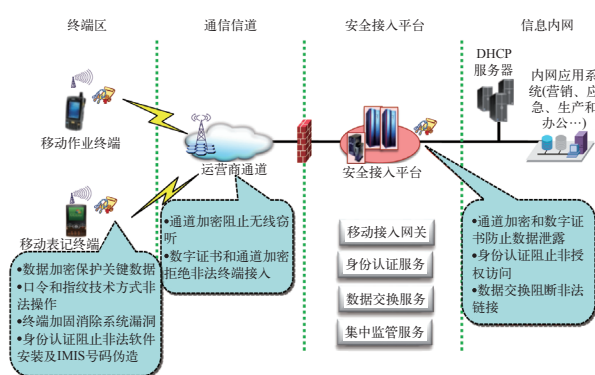


图2 业务数据接入公司信息内网时采取的安全措施

装信息隔离装置进行数据双向隔离，保障信息安全，如图3所示。

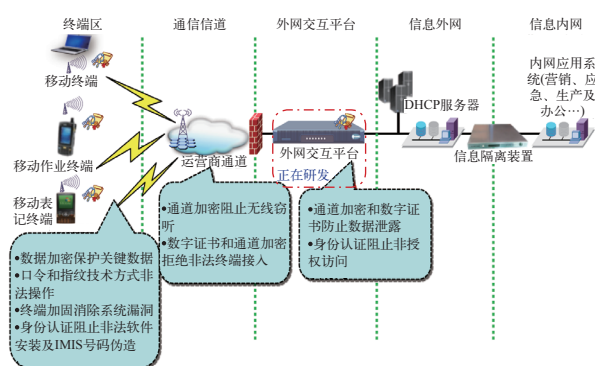


图3 信息隔离装置机制说明

3 无线公网攻击监测技术

配用电无线公网网络环境认知攻击检测的主要实现方法是在网络运行过程中节点随环境的变化随时根据需要插入新的攻击检测代码，目前无线公网中常见的攻击如图4所示。

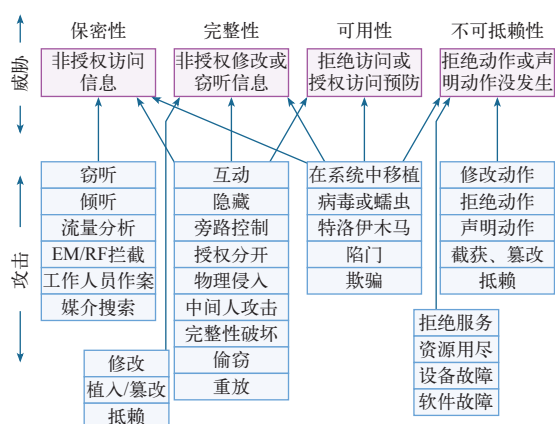


图4 常见网络攻击分类

支持代码动态加载的典型中间件有Mate、Sensor Ware和Agilla。拟采用人工智能中的“认知”的思想，设计灵活的环境认知攻击检测模型。该模型按照感知—判断—行动的认知过程进行无线自组织网络的攻击检测代码更新，如图5所示。用基于规则的知识表示环境信息，通过规则推理分析环境的变化，进而决定与当前环境相匹配的攻击检测代码。

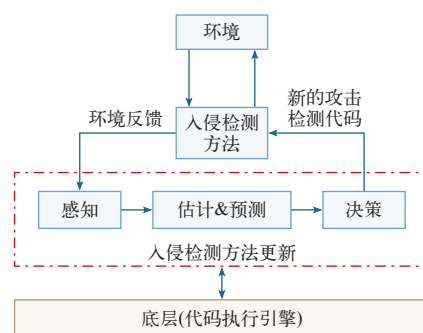


图5 无线网络环境认知的攻击检测过程示意图

配用电无线通信网络的攻击检测机制涉及的功能实体有配电终端节点、用电终端节点、网关节点和监控中心。

1) 配用电终端节点。内置节点本地攻击检测功能。

2) 网关节点。内置数据汇聚攻击检测功能，负责收集由配用电终端节点传来的各种数据信息以及网络节点列表，该列表包括该网关节点所负责管理区域中的所有网络节点，该网关节点还能处理配用电终端设备节点传送过来的数据信息和上报信息，并基于机器学习算法进行决策，进而更新节点上的攻击检测代码。

3) 监控中心。采集各网关节点上报的攻击检测信息，进行综合分析与安全评估。

该入侵检测方法可以由数据采集、数据分析、触发判断和新攻击代码分发四个部分组成。其中数据采集和数据分析功能部署在配用电终端节点上；触发判断部署在网关节点上，新攻击代码分发需要网关节点和终端节点配合完成。

3.1 基于生物启发的攻击检测算法

本文选择采用双重检测器的阴性选择算法异

常检测系统黑洞覆盖优化算法模型（DLD-NSA模型），这种算法能够有效地改善黑洞元素检测率，并且这种算法在检测速率方面，相比于其他算法来说，其检测速率更有优势。阴性选择算法包括生成检测器集合和测试待检数据两个阶段：①生成检测器集合，检测器是随机生成的字符串，与任意的自我元素都无法匹配；②使用检测器集测试待检数据，如果匹配结果为“匹配”，那么可以判定这是非我/有害数据。

基于阴性选择算法的DLD-NSA模型，如图6所示。

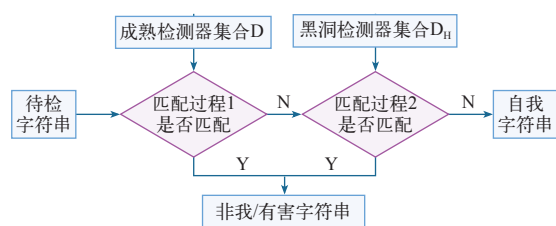


图6 DLD-NSA模型攻击检测算法

从危险理论中可以得知，受难细胞会产生并向输出一种危险状态信号，与此同时，该细胞的活动区域附近会自动构建一个危险区域，APC捕获其中的抗原后会提呈抗原，并提供一种共同刺激信号，这就引发了免疫应答。在免疫应答的过程中，淋巴细胞会生成一种抗体，这种抗体与危险区域里面的抗原是匹配的^[5]。借助危险理论的工作机理，这一检测过程由三部分组成，其中包括危险感知阶段、抗原提呈阶段和决策阶段，如图7所示。

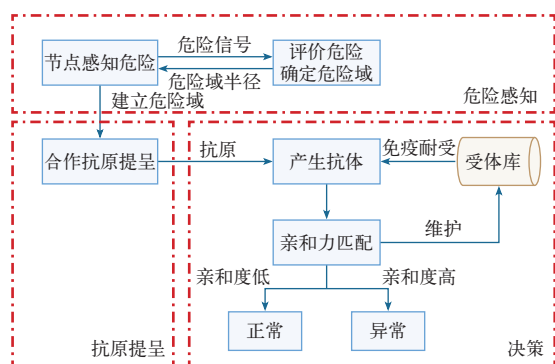


图7 基于危险理论的攻击检测模型

危险理论在人工免疫系统中并不简单，如果把危险理论全部挪用到攻击检测系统中，这种做

法的意义不大。这种攻击检测算法借鉴了自然生物免疫系统的工作机制，为了能够适用于攻击检测系统，将危险理论进行简化和抽象处理后，才在无线公网的攻击检测系统中使用危险理论。表2为基于危险理论的简明受伤分级（AIS）到配用电无线专网的攻击检测建模关系。

表2 危险理论AIS到攻击检测系统算法的建模

免疫系统	配用电无线专网攻击检测模型
淋巴细胞	网关节点和监控中心
病原体	攻击节点或者具有传播性的蠕虫、病毒
凋亡细胞	由于硬件故障等原因正常不工作的终端节点
受难细胞	细胞遭受了攻击，从而产生危险感知的终端节点
危险信号	向网关节点传递信息，这个信息告知网关节点有潜在入侵
APC	处于危险区域中的节点，合作起来提供抗原
抗原	危险域中的全局信息
抗体	由耐受过程产生的异常模式
受体	由受体组成为抗原和抗体，每一个受体描述了关于每个节点的流量信息的正常模式

3.2 基于相似度的攻击检测算法

针对配用电无线公网通信网络中物理层的信道阻塞干扰入侵、链路层的数据碰撞入侵、网络层的RREQ泛洪入侵以及应用层的感知数据篡改入侵的核心特征，提出一种基于相似度计算的攻击检测模型，通过相似度算法来衡量特征向量之间的相似程度，同时为了减小检测的误检率和漏检率，提出等级判别标准，对可疑行为与实时数据的联系进行趋势判别。

(1) 入侵行为特征分析

配用电网无线自组织网络中不同协议层中存在多种入侵行为，而不同的入侵行为之间的特征存在一定的差异，选择其中较为突出的入侵行为特征作为网络攻击检测指标能够快速高效地发现网络中出现的异常行为，同时也能有效分配网络资源。各种入侵行为的典型特征描述如表3所示。

(2) 基于相似度计算的入侵检测模型

一种与相似度计算有关的算法能够实时检测，该算法通过计算相似度来实现攻击检测，该算法主要是对网络中的所有当下行为进行解析，然后提取出行为特征，根据行为特征来判别某一行为属于入侵行为还是正常行为，基于传统的监

表3 无线自组织网络入侵行为的详细描述

入侵种类	所在协议层	行为描述	代表特征
RREQ	网络层	恶意节点伪装为合法节点，向网络其他节点持续广播RREQ路由请求，导致网络中的大部分节点由于长时间持续相应路由请求导致能源耗尽、无法提供正常服务，破坏网络的可用性	RREQ接收
			RREQ发送
			RREQ错误比例
数据包碰撞	链路层	恶意节点会时刻监听通信网络中传输的信息，如果发现数据包，恶意节点就会发出一种无效数据包来，通过与正常的数据包进行碰撞，导致发送节点发送失败，使得网络节点长时间处于无法成功通信的状态，造成DDOS攻击效果	延迟时间
信道干扰	物理层	恶意节点通过信道扫描发现目标网络工作信道后，对目标网络的工作信道采取多种类型的信道干扰	延迟时间

督学习方法的算法准确性取决于训练库，然而该算法并不受训练库的影响，而且更改了之前的相似度判别模型^[6]，提出一种基于相似度计算的检测方法，如图8所示。这种方法能够应对不同的环境状况。该入侵检测模型存在双重检测模块，其中第一层检测模块为相似度检测模块，第二层为行为趋势判别检测模块。

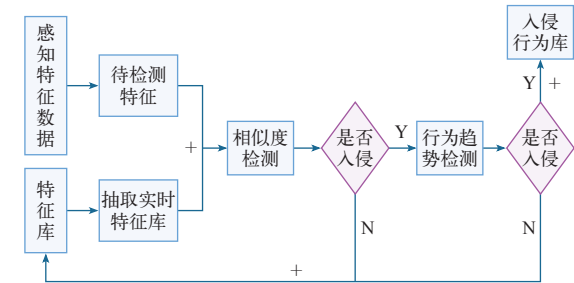


图8 基于相似度的攻击检测算法结构图

基于相似度的攻击检测模型分为数值感知中心和数据检测中心，如图9所示。数值感知中心由感知层特征提取模块组成，检测中心主要由特征库模块、入侵检测（包括相似度检测单元和行为趋势检测单元）和入侵行为库模块组成。感知层特征提取模块主要负责对各个网络节点进行数据采集，对采集回来的网络数据进行数据分析，然

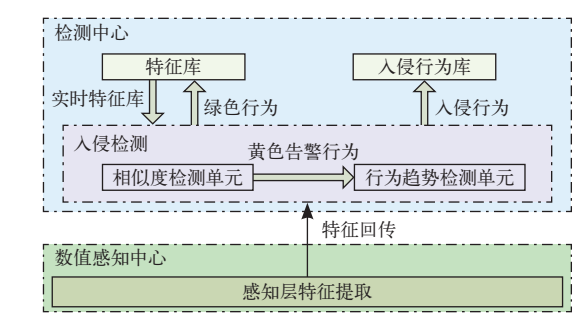


图9 基于相似度的攻击检测算法模型

后经过特征提取处理后再传输给检测中心进行下一步分析。

4 结束语

本文针对配电网无线公网接入的安全问题，结合基于相似度的攻击监测和生物启发式的攻击监测方法，来及时发现并处理无线公网中常见的一些诸如DDOS、蠕虫攻击等网络攻击，从而保证配用电通信业务的数据安全和传输安全。

参考文献

[1] 雷煜卿, 李建岐, 侯宝素. 智能配用电通信网架结构[J]. 电力系统通信, 2011, 32(6): 73-78.

[2] 权楠, 雷煜卿, 黄毕尧, 等. 智能电网下的电力终端通信接入架构研究[J]. 电力系统通信, 2012, 33(1): 74-77.

[3] 曹津平, 刘建明, 李祥珍. 面向智能配用电网络的电力无线专网技术方案[J]. 电力系统自动化, 2013, 37(11): 76-80.

[4] Dogman A, Saatchi R, Al-Khayatt S. Evaluation of computer network quality of service using neural networks[J]. 2012 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA), 2012; 217-222.

[5] 郑瑞娟. 生物启发的多维网络安全模型及方法研究[D]. 哈尔滨: 哈尔滨工程大学, 2008.

[6] 钟敦昊, 张冬梅, 张玉. 一种基于相似度计算的无线传感器网络入侵检测方法[J]. 信息安全, 2016(2): 22-27.

(收稿日期: 2018-01-02) EA