文章编号:2095-476X(2015)5/6-0088-05

智能电网中分层网络结构的入侵检测系统研究

徐静[1], 姚志垒[2], 徐森[1], 李永忠[3], 吴素芹[1]

(1.盐城工学院 信息工程学院, 江苏 盐城 224051;
2.盐城工学院 电气工程学院, 江苏 盐城 224051;
3.江苏科技大学 计算机科学与工程学院, 江苏 镇江 212003)

摘要:为了提高智能电网的安全性和可靠性,将入侵检测系统运用到智能电网中.针对智能电网具有网络节点多、信息传输量大、安全要求高等特点,提出一种基于多Agent的入侵检测系统模型,并将该模型部署到智能电网的分层网络结构中,以减少数据传输,节约带宽,解决速度瓶颈问题;针对入侵检测的误检率高、漏检率高等问题,提出适合智能电网的动态克隆选择算法,将所提算法与多Agent技术相结合,构造了具有免疫功能的Agent.利用标准的入侵检测测试数据集——KDD'99数据集——对所提模型和算法进行仿真验证,结果表明:本系统在保证低误检率的同时,提高了智能电网中常见的Dos和Probing类型攻击的检测率.

关键词:智能电网;入侵检测;多代理;动态克隆选择算法
中图分类号:TP309 **文献标志码**:A **DOI**:10.3969/j.issn.2095-476X.2015.5/6.018

Research on intrusion detection system in hierarchical network architecture of smart grid

XU Jing[1], YAO Zhi-lei[2], XU Sen[1], LI Yong-zhong[3], WU Su-qin[1]

(1. *School of Information Engineering, Yancheng Institute of Technology, Yancheng* 224051, *China*;
2. *School of Electrical Engineering, Yancheng Institute of Technology, Yancheng* 224051, *China*;
3. *School of Computer Science and Engineering, Jiangsu University of Science and Technology, Zhenjiang* 212003, *China*)

Abstract: In order to improve the safety and reliability of the smart grid, the intrusion detection system was applied to the smart grid. As smart grid had the characteristics of large number of network nodes, large amount of information transmission and high safety requirements, an intrusion detection model based on multi-agent was established, and was deployed in the hierarchical network structure of smart grid. Therefore, amount of transmission data was reduced, bandwidth was saved and speed bottleneck problem was solved. With the purpose of reducing false positive rate and false negative rate in current intrusion detection system, dynamic clonal selection algorithm for the smart grid environment was proposed. The proposed algorithm could be combined with the multi-agent technology, the immune agents were constructed. The proposed model and algorithm were simulated by KDD'99 datasets. Simulation results showed that the proposed system had low false positive rate and improved the detection rate of Dos and Probing attack that are common attack in smart grid.

收稿日期:2015-05-18
基金项目:国家自然科学基金项目(51407153)
作者简介:徐静(1981—),女,江苏省盐城市人,盐城工学院讲师,主要研究方向为智能电网与入侵检测.

Key words: smart grid; intrusion detection; multi-agent; dynamic clonal selection algorithm

0　引言

为了解决能源安全、气候变化和经济增长等全球性问题,迫切需要加速低碳能源技术的发展. 智能电网可以使能源供应顺应能源需求,从而满足供应安全和低碳排放的需要[1]. 智能电网是一个完全自动化的电力传输网络,能够监视和控制每个用户和电网节点,保证从电厂到终端用户整个输配电过程中所有节点之间的信息和电能的双向流动[2]. 智能电网分为 3 层[3],分别为家庭网络 HAN(home area network)、邻域网络 NAN(neighborhood area network)、大电网 WAN(wide area network).

信息化是实现智能电网基础功能的重要前提,但信息化给智能电网的安全运行和数据隐私保护带来了许多问题[4],主要有:

1)当 WAN 层受到攻击时,不法分子能直接控制电网的运行,从而导致整个电网的瘫痪.

2)当 NAN 层受到拒绝服务攻击 Dos(denial of service)时,相关的数据信息将被延迟、阻塞,甚至破坏. WAN 层将不能及时获得电网当前状态的信息,从而不能准确地进行分析、判断及决策. 例如:在电动汽车入网时受到 Dos,电动汽车充放电不能被合理安排以适应当前电网状况,反而会加重电网的负荷;用户不能及时得到车辆车能状况、电网负荷状态和计费信息等,从而不能充分利用分时电价对智能家电进行充放电.

3)当 NAN 层受到其他类型攻击时,数据被篡改,将可能导致 WAN 层的决策错误,从而严重危害电网的稳定运行.

4)HAN 层每个用户需要共享他们使用能源的信息,而每个用户的用电负荷、设备构成及用电规律等个人隐私将暴露在信息网上,这些信息有可能会被不法分子截获、篡改甚至用于其他非法用途.

入侵检测系统 IDS(intrusion detection system)作为一种主动的网络安全防御措施[5-7],可以实时监控网络中各节点的运行情况,对信息的采集、传输、处理和交互等各个环节加强保障,及时发现异常,并迅速响应,防止攻击者的非法入侵,提高网络的可靠性、可用性和综合效率. 2010 年,R. Berthier 等[8]受 IT 中安全防护措施的启发,提出智能电网中除了要有安全协议和实施强有力的安全属性外,还需对网络中传输的数据进行实时监控并分析,及时检测入侵行为. 他们将入侵检测应用在智能电网中,以防止智能电网中的高级测量体系遭到攻击. 文献[9]提出一种智能电网中基于 HAN 层的入侵检测系统,检测算法是基于异常的检测,对已知攻击有较好的检测能力,但对未知的攻击的检测能力较差. 文献[10]提出一种针对智能电网中 NAN 层的入侵检测系统,该系统对 NAN 层的蠕虫攻击具有一定的检测能力. 但上述文献都仅针对智能电网中的某一层设计入侵检测系统,无法保证对整个智能电网的实时监控.

为了提高智能电网的安全性和可靠性,本文将入侵检测系统部署到智能电网的各层中,实时监控和分析智能电网中传输的数据,针对智能电网节点多、数据传输量大的特点,引入多 Agent 技术到入侵检测中,构建智能电网环境下的基于多 Agent 的入侵检测模型,以减少数据传输,节约带宽,解决瓶颈问题;针对现有入侵检测系统误检率高、漏检率高的问题,提出一种适合智能电网的动态克隆选择算法,以提高对已知和未知攻击的检测率. 利用 KDD'99 数据集对所提模型和算法进行仿真验证.

1　系统设计

1.1　智能电网分层结构

智能电网的分层架构见图 1. 其中,HAN 对应电力网中的用户,NAN 对应电力网中的配电,WAN 对应电力网中的输电和发电[3]. 图 2 是智能电网中分层网络结构的内部框图. 其中,HAN 把家庭网关与用户户内可控的智能电器或装置连接起来,用户通过智能电表查看电表的值和电力公司当前的价格信息,根据需要或市场的需求调整用电习惯;NAN 连接电表与采集器;WAN 连接家庭网关与数据采集平台[11].

根据智能电网中 HAN,NAN 和 WAN 各层之间双向传输的特点,将入侵检测系统部署到图 1 的各网络层中. 下面将分别对该入侵检测系统的模型和算法进行阐述.

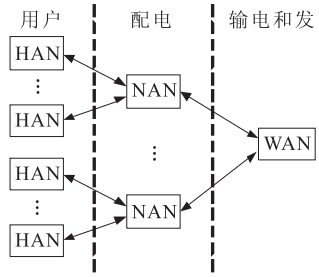

图 1　智能电网的分层架构图

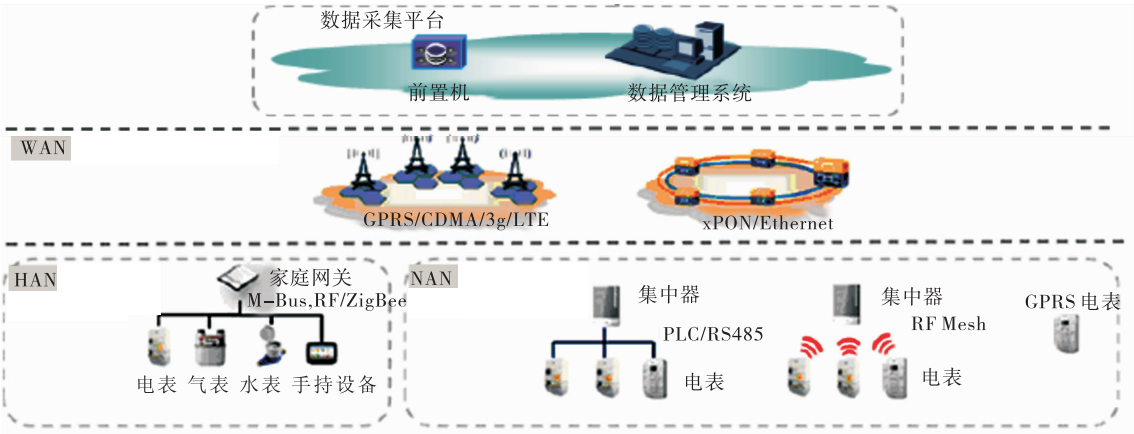

图 2 智能电网各层的内部结构图

1.2 基于多 Agent 的入侵检测模型

基于多 Agent 的入侵检测模型由具有不同功能的 Agent 构成,系统中所有的 Agent 按其功能可分为 4 类:控制 Agent,采集 Agent,检测 Agent 和响应 Agent. 通过派遣和移动各功能 Agent 取代传统的大量待检测数据的传输,减少数据传输量,解决瓶颈问题. 其体系结构如图 3 所示.

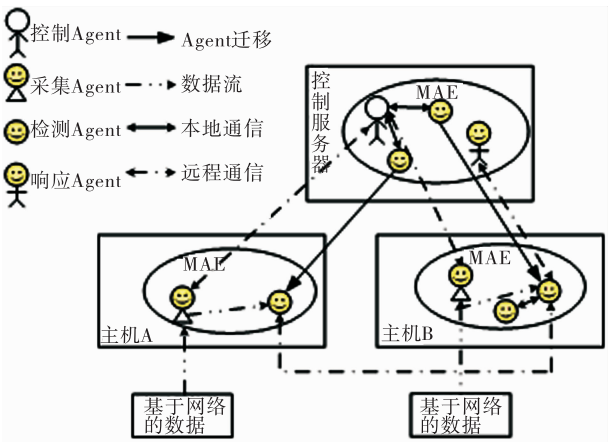

图 3 基于多 Agent 的入侵检测模型

控制 Agent:主要负责管理、协调、控制被监控主机上的 Agent,生成带检测器的检测 Agent,收到采集 Agent 的信号之后,派发检测 Agent 到相应的主机中. 检测 Agent 产生之后,其工作过程是独立的,与控制 Agent 无关,即使控制服务器受到攻击,也不会影响已经产生的在系统内的检测 Agent. 检测 Agent 可以通过克隆,移动到需要检测的主机上进行检测,可为恢复控制平台的工作争取时间,消除中央控制器的单点失效问题.

采集 Agent:分布在网络中的各重要节点上,主要负责对网络数据包的截获和对截获的网络数据包进行预处理,由于采集到的数据信息量非常大,所以采集 Agent 要过滤出相关的信息,减少无用的信息入库,并对其进行编码,将数据提供给检测模块进行检测分析.

检测 Agent:检测部分是整个入侵检测的核心. 主要完成对采集 Agent 预处理的数据进行检测分析. 检测器分为未成熟检测器、成熟检测器和记忆检测器,将成熟检测器和记忆检测器嵌入到 B-Agent 和 M-Agent 中(如图 4 所示). B-Agent 和 M-Agent 可以在主机间迁移,相互进行通信协作,以完成检测.

响应 Agent:当 B-Agent 或者 M-Agent 检测到有入侵或可疑行为时,它们便及时激活响应 Agent,立即发出警报,并对此做出响应.

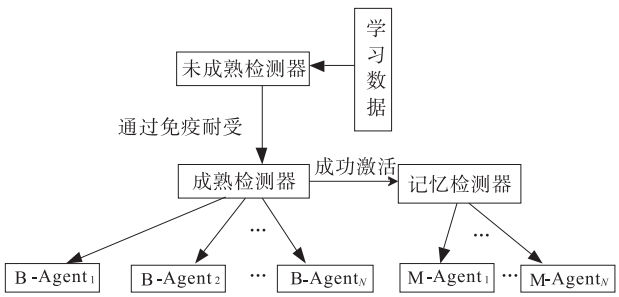

图 4 检测器分类图

1.3 适合智能电网的动态克隆选择算法

文献[12]提出基于动态克隆选择算法的入侵检测系统,该算法可以提高系统的检测率,降低误检率和漏检率. 但由于智能电网动态的网络环境和大量信息交互,入侵检测系统中的检测器集合不可能覆盖整个抗原空间,本文提出一种适合智能电网的动态克隆选择算法,每 N 代更换 1 个由自我抗原

群体和非我抗原群体构成的簇,一次针对自体集的 1 个子集进行耐受学习,并且当网络环境发生变化时,替换过时的检测器.

适合智能电网的动态克隆选择算法伪代码为

```
Generation_Number = 1;
while( Generation_Number < = 最大迭代次数){
  if( Generation_Number% N = = 1)
    选择新的抗原簇;
  未成熟检测器耐受阶段
  成熟检测器学习阶段
  记忆检测器学习阶段
  Generation_Number + + ;
}
```

其中,未成熟检测器耐受阶段伪代码为

```
while( immature_detector! = null){
  if( 该检测器与自我抗原集中自我抗原匹配)
    删除该检测器;
  else{
    该检测器加入到未成熟检测器中;
    immature_age + + ;
  }
  if( immature_age > = T){
    将该未成熟检测器加入到成熟检测器中;
    将该检测器从未成熟检测器集中删除;
    }
}
```

```
While( 成熟检测器个数 + 未成熟检测器个数 < 非记忆检测器的最大值){
      随机生成检测器加入到未成熟检测器集中;
    }
```

成熟检测器学习阶段伪代码为

```
while( mature_detector! = null){
  Mature_age + + ;
  if( 有抗原与该成熟检测器匹配{
    if( 抗原与当前 self 集匹配){
      从成熟检测器集中删除该检测器;
      将该抗原放入到 self 集中;
    }
    else{
      删除该抗原;
      Mature_count + + ;
    }
  }
  if( mature_count > = A){
    将该检测器加入到记忆检测器集中;
    将此检测器从成熟检测器集中删除;
  }
  else{
    if( mature_age > = L)
      删除该成熟检测器;
    }
  }
```

记忆检测器学习阶段伪代码为

```
while( memory_detector! = null){//记忆检测器非空
  if( 有抗原与该记忆检测器匹配){
    if( 该记忆检测器与当前 self 集匹配){
      删除该记忆检测器;
      把该抗原加入到 self 集合中;
    }
    else 删除该抗原;
  }
}
```

该算法的伪代码中,参数 T 表示未成熟检测器的耐受期,参数 L 为成熟检测器的生命周期,参数 A 为成熟检测器的激活阈值. 所提算法中的匹配是指两字符串连续 r 个属性相同.

2　仿真验证与分析

以 KDD'99 数据集中的 kddcup. data_10_percent 数据作为学习数据,选取数据集中标记为 normal 的数据作为自我耐受学习,攻击数据作为检测器学习所用数据. 测试所提模型和算法的检测性能则用其中的 corrected 数据集,corrected 中除包含在 kddcup. data_10_percent 中出现的 20 种攻击外,还有 17 种未出现过的攻击. 将本文算法与文献[12]算法检测性能相比较,其结果见图 5.

由图 5 可知,本文所提算法在具有较高检测率的同时,对学习过程中未出现的攻击也具有一定的检测能力. 对于智能电网中出现较多且致命的 Dos 和 Probing 两种类型的攻击检测性能较高. 对于 U2R 和 R2L 两种类型的攻击检测率低的原因主要是在学习阶段针对这两种攻击特征的学习样本较少,很难形成针对这两种攻击的检测器.

更重要的是,所提模型充分利用 Agent 的移动

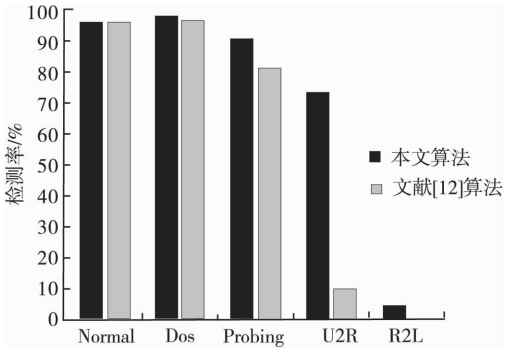

图 5 不同算法检测性能

性,实现分布式数据采集预处理及检测分析,因此不会由于引入入侵检测系统而加重智能电网的传输负担.

3 结语

本文利用 Agent 的移动性和协作性,结合免疫原理,提出智能电网中的基于多 Agent 的入侵检测系统模型和适合智能电网特征的动态克隆选择算法,并在 KDD'99 数据集上进行验证,结果表明本文提出的方法除了能检测已知攻击外,对未知攻击也具有一定的检测能力,提高了智能电网中常见且致命的 DOS 和 Probing 两种类型攻击的检测率. 针对 U2R 和 R2L 类型检测率低,下一步的工作目标是在智能电网中采用 PKI 认证技术来降低本地超级用户的非法访问和未授权的远程访问对智能电网所带来的影响.

参考文献:

[1] Farhangi H. The path of the smart grid[J]. IEEE Power and Energy Magazine,2010,8(1):18.

[2] 何光宇,孙英云,梅生伟,等. 多指标自趋优的智能电网[J]. 电力系统自动化,2009,33(17):1.

[3] Kuzlu M,Pipattanasomporn M,Rahman S. Communication network requirements for major smart grid applications in HAN,NAN and WAN[J]. Computer Networks,2014,67:74.

[4] McDaniel P. Security and privacy challenges in the smart grid[J]. IEEE Security and Privacy,2009,7(3):75.

[5] 许颖梅. 基于 Web 数据流技术的网络入侵检测研究[J]. 郑州轻工业学院学报:自然科学版,2012,27(3):11.

[6] 王汝传,王华,徐小龙. 基于移动代理的入侵检测系统模型的研究[J]. 通信学报,2004,25(1):22.

[7] 王晋,李德全,冯登国. 一种基于移动代理自动优化的分布式入侵检测系统[J]. 计算机研究与发展,2006,43(1):9.

[8] Berthier R,Sanders W H,Khurana H. Intrusion detection for advanced metering infrastructures: requirements and architectural directions[C]// IEEE International Conference on Smart Grid Communications,Piscataway: IEEE,2010:350 – 355.

[9] Jokar P,Nicanfar H,Leung V C M. Specification-based intrusion detection for home area networks in smart grids[C]// IEEE International Conference on Smart Grid Communications,Piscataway:IEEE,2011:208 – 213.

[10] Beigi-Mohammadi N,Misic J,Khazaei H,et al. An intrusion detection system for smart grid neighborhood area network[C]// IEEE International Conference on Communications,Piscataway:IEEE,2014:4125 – 4130.

[11] 张磊,侯超,翁新瑜. 用电信息采集系统通信技术应用研究[EB/OL]. http://www.gridsources.com/contents/2383/407386.html,2013 – 01 – 06.

[12] Jungwon K,Bentley P J. Towards an artificial immune system for network intrusion detection: An investigation of dynamic clonal selection[C]// Proceeding of the 2002 Congress on Evolutionary Computation,Piscataway:IEEE,2002:1015 – 1020.