通讯与网络

灰色关联算法在物联网安全状态评估中的应用

Study of the application for the security state assessment about the internet of things based on grey correlation algorithm

高洪波

GAO Hong-bo

（江苏城市职业学院 南通校区 电信系，南通 226006）

摘 要：网络安全状态评估是网络安全领域的研究热点之一，其中分析某时段网络系统所处的安全状态是主要研究方法之一，其目的是为管理者提供管理决策。灰色关联算法是一种非常适合动态运行系统的分析算法。随着物联网在各行各业中全面推进，安全问题成为了其要解决的关键问题。文章在探讨物联网存在的主要安全问题的基础上，探讨了基于灰色关联算法的物联网安全状态的评估方法，并进行了相应的实证分析。

关键词：物联网；安全；评估；灰色关联算法

中图分类号：TP301.6 **文献标识码**：A **文章编号**：1009-0134(2012)11(下)-0023-03

Doi: 10.3969/j.issn.1009-0134.2012.11(下).07

0 引言

对网络安全状态进行科学准确评估是保证网络安全运行的重要手段之一。如何通过广泛的搜集网络运行中的有关数据信息，依据科学的算法来反映评估对象的网络安全的基本面貌和水平是近年来热议的话题。随着计算机通信技术的飞跃式发展，网络信息安全的内涵和外延不断地延伸，用翻天地覆的变化来形容也毫不夸张。主要体现在：从最初的侧重于信息保密性发展到如今网络安全信息的完整性、可用性、可控性和不可否认性，其主要技术和理论为“攻击、防范、检测、控制、管理、评估”等六方面，目的是构建网络信息安全的“攻、防、测、控、管、评”立体式防范体系。其中网络信息安全风险评估是保障网络信息安全和正常运行的基础和手段。绝对的安全是不存在的，但通过科学准确的网络信息安全风险评估可以进一步降低安全风险，从而为网络信息提供者、使用者判定网络安全状态，保障信息安全提供支撑。可见，网络信息安全状态评估是网络信息安全得以保障的重要基础性工作之一。

近年来，随着信息技术的飞速发展，物联网正在成为世界各国信息产业的重要组成部分，它的出现和广泛推广应用已成为推动信息技术在各行各业进一步深化应用的强有力的推动力。较之于互联网安全问题，物联网的安全问题显得更加突出。互联网遭受到安全威胁时通常造成的是信息资产领域的损失，而物联网一旦遭到致命的攻击，则会直接对人们的工作和生活甚至是对整个国民经济造成巨大的影响。与互联网相比，物联网涉及社会经济的各个层面，具有更大的市场价值，可以预见，攻击物联网对那些为谋取私利的不法之徒将会更具诱惑力。因此，随着物联网在各行各业的普及和推广，物联网将面临着更为严峻的安全挑战。所以，对物联网进行安全状态的评估进而保障其安全运行就显得十分的重要和具有深刻的现实意义。

1 物联网信息安全面临的问题和特点

1）物联网来源于互联网，具有互联网同样的先天不足的特性而导致其存在一定的安全问题。

2）更为复杂的网络环境使得物联网信息安全的保障较为困难。物联网将网络的概念扩展延伸到了现实工作、生活的各个领域，可以说人们的现实工作、生活将建立于物联网之上，这种物联网的复杂性势必带来了许多不确定性因素，复杂

收稿日期：2012-06-11

作者简介：高洪波（1965-），男，江苏泰州人，副教授，硕士，主要研究方向为计算机信息安全与数据挖掘。

性是物联网安全难以控制的主要问题之一。

3）物联网开放的无线信道使其很容易受到外部信号干扰和攻击；另外，无线信道没有明显边界使其很容易被监听。

4）物联网终端由于其一般采用的是微型传感器，处理、存储能力以及能量都比较低，造成对一些计算、存储、功耗要求较高的安全措施无法实施和加载。

5）随着对无线终端和无线网络等攻击技术不断发展，无线网络比有线网络更容易受到入侵，要使物联网真正高效安全，在信息安全保障措施方面需要比传统的互联网更进一步的加大力度。而加大对物联网安全状态的评估力度，借助科学高效的算法确定实时的安全状态，是保障物联网安全的重要举措之一。

综上所述，物联网面临的安全问题是管理者必须高度重视和认真面对的。要解决物联网安全问题就必须避免重蹈传统互联网的覆辙，即在搭建和管理物联网时，要有全局“一盘棋”思想，从整体、系统的角度来思考，从物联网终端、无线传输、互联网传输的各个环节全面地考虑安全性，力争将安全问题解决在设计之初。

2 物联网安全状况评估的必要性

随着信息时代的到来和 Internet 的迅速发展，各种网络攻击事件的屡屡发生，网络信息安全问题已成为备受关注的焦点。为了保证网络安全运行，现在管理者通常采用了入侵检测、防火墙、病毒检测等技术。然而借助这些技术每天都会产生近乎于海量的网络信息，使得网络管理者很难真正全面地了解网络系统的真实安全状态，太多的信息有时使管理者不能及时采取恰当的对策。因此如何真实、准确、客观地对网络运行安全状况进行科学准确的评估就显得尤为重要。

网络安全状态分析通常包括某时刻各种网络设备运行情况、网络服务状况及用户行为分析评估等几个方面。在物联网这种大规模网络环境中，对引起网络安全状况发生变化的安全因素进行提取、分析、显示，从而达到预测未来发展的趋势的目的，是物联网安全状态评估的关键之一。而要达到此目的，采用科学高效的算法来处理和融合海量的网络安全状态数据就显得十分的必要。

鉴于此，本文将灰色系统理论引入物联网安全状态的评估中，把常见的几种网络攻击行为作为安全因素，通过使用灰色关联分析法来量化某段时间内网络攻击行为对该网络所产生的相对影响，进而实现对整个网络所处的安全环境与状态的定量评估，达到帮助物联网管理者更好地管理好网络，使其真正发挥应有的作用的目的。

3 灰色关联分析法基本思想

灰色关联分析法的基本思想是：在众多客观事物及纷杂的因素之间，存在着大量的、相互交错的复杂关系，人们在分析和决策时，经常是处于难以得到全面、足够的信息和形成明确的概念的境地，诸如此类往往是灰色因素在起作用，因此对灰色系统进行分析和研究时，解决此类问题的关键是如何从随机的时间序列中，找到关联性和关联性的度量值，以便进行因素分析，为决策提供依据。灰色系统理论提出了对其各子系统基于灰色关联度分析的方法，其目的是通过一定的方法，来寻求整个系统中各子系统或因素之间的数值关系，这种关联性的度量值通常称为灰色关联度。基于灰色关联度分析对于一个系统发展变化状态可以提供量化的度量分析，非常适合动态运行系统的分析。物联网作为实时动态的系统，运用灰色关联法来分析其网络安全状态具有较好的可操作性和实用价值。

4 基于灰色关联算法的物联网信息安全状态评估具体步骤

下面给出基于灰色关联算法的物联网信息安全状态评估具体步骤：

1）收集和统计检测考察时间段 T 内的网络受到的攻击数据。根据整个系统的性能和实际情况，时间段 T 的大小可作相应的调整。网络所遭受的攻击的种类通常可分为 Ping 攻击、RPC 攻击、DOS 攻击、Shellcode 攻击、DNS 欺骗和 http 攻击等。同时在表 1 中选取各种攻击类型统计数据中最小值作为理想参考数列。

2）将上述所统计的数据表进行无量纲化处理，并根据相关公式求取其灰色关联矩阵（限于篇幅公式此处略），得到其相关的灰色关联系数值。

3）根据上述各种攻击危害性，结合专家系统给出的权重，计算出网络安全状态指数值。

4）依据上述得到的网络安全指数值分析得出网络的安全状态。

5 实证分析

1) 收集和统计检测考察时间段 T 内的攻击数据。

表 1 是某物联网在一段时间内受的攻击类型和次数，表中统计了在 T 时间内物联网某一关键网段所遭受的攻击情况。如表 1 所示，其中 A1 是 Ping 攻击，A2 是 RPC 攻击，A3 是 DOS 攻击，A4 是 Shellcode 攻击，A5 是 DNS 欺骗，A6 是 http 攻击。表 1 中的数据是检测到的各种攻击类型在相应的时间段 T1 ～ T8 中的次数。

表1 遭受的攻击类型次数和理想参考数列

时间段	A1	A2	A3	A4	A5	A6
T1	40	0	0	2	3	2
T2	0	18	90	8	27	0
T3	1	1	1	0	6	28
T4	0	0	0	0	144	0
T5	8	0	160	1	28	0
T6	50	50	120	9	280	15
T7	45	25	50	0	72	15
T8	0	6	15	0	40	14
参考数列	0	0	0	0	3	0

2) 将表 1 中的数据无量纲化处理，并根据相应得公式求出其灰色关联矩阵，得到相关因素的灰色关联系数值，如表 2 所示。

表2 灰色关联系数值

时间段	A1	A2	A3	A4	A5	A6
T1	0.77591	1	1	0.985767	0.978799	0.985795
T2	1	0.884984	0.606127	0.945393	0.868339	1
T3	0.992832	0.992832	0.992832	0	0	0.831832
T4	1	1	1	1	0.500904	1
T5	0.945393	1	0.463987	0.992832	0.862928	1
T6	0.734748	0.734748	0.535783	0.938983	0.335758	0.90228
T7	0.754768	0.847095	0.734748	1	0.677262	0.90228
T8	1	0.958478	0.90228	1	0.802899	0.908197

3) 根据上述各种攻击危害性的权重进而计算网络安全风险指数值。

依据各种攻击危害性对网络系统安全影响，结合专家系统选取权重，此处对于上述的 6 种攻击对应的权重选取如下：

V = {0.250，0.0833，0.250，0.250，0.0833，0.0833}，

4) 依据上述权重及得到的灰色关联系数得出网络的安全状态指数值，计算结果见表 3。

表3 各时段网络安全状态指数值

时间段	T1	T2	T3	T4	T5	T6	T7	T8
指数制	0.937367	0.867232	0.981710	0.958382	0.839035	0.716712	0.824518	0.947946

通过对表 3 的各时段网络安全状态指数值分析可以看出，该网络在时间段 Tl、T3、T4、T8 内的安全指数值比较大，表明在这些时间段内网络的状态比较安全、稳定；在时间段 T2、T5、T7 内虽然遭受到一定的威胁，但还可以维持其正常的运行状态，而对于 T6 时间段，网络安全指数值比较小，表明这个时间段内网络遭受的威胁较之于其他时间段要高，应该引起网络管理者的高度重视，采取必要的防范措施。

通过上述实例可以看出用本文给出的基于灰色理论的物联网安全状态评估方法得出的评估结果与实际情况还是比较符合的。即与表 1 中从直观上判断，也可以看出的确在时间段 T6，网络处于较高的受威胁状态。

6 结束语

随着物联网技术的广泛推广和运用，和任何一次新技术的产生一样，将在社会生产、生活的各个方面产生广泛而深入的影响。但同时我们也应看到在物联网显著提高经济和社会运行效率的同时，其对国家和公民的机密、信息安全和隐私保护等方面的安全问题提出了严峻挑战。我国物联网的发展仍处于起步阶段，有关物联网信息安全防护问题的研究任重道远。本文通过较为详尽的对物联网安全问题的探讨，结合灰色关联算法提出了物联网安全状态评估的方法和步骤，并通过实证分析，说明了灰色关联算法在物联网安全状态评估中运用的具体过程，对在实际应用

【下转第29页】

4.4 传感器的灵敏度控制

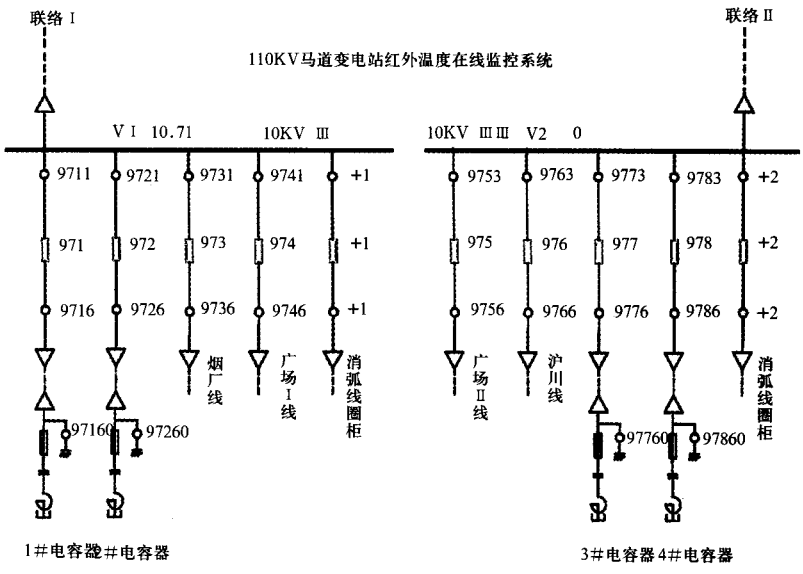

图6 监测软件的实时传感数据

传感器的灵敏平衡度是通过测量每边的灵敏度（即单边输出峰值电压），并采用下列公式计算得出。

$$平衡度=\frac{|VA-VB|}{VA+VB}\times 100\% \qquad (6)$$

式中，VA 为 A 面的灵敏度，VB 为 B 面的灵敏度。

5 结束语

该系统通过对温度状态的监测实现了对设备的运行状态监测。系统通过对采集到的数据进行科学分析、深度挖掘从而指导设备运行，尤其对负荷的变化进行科学指导，变被动检测为主动监测，使电力系统对设备运行管理做到既科学又安全，为生产管理及运行决策提供参考依据，提高电力系统的运行水平[9]。

本系统的运行可及时发现故障隐患并发出报警及检修建议，使被动检测变为主动监测，将故障消灭在萌芽状态，减少事故的发生，也使检修工作变得更加有目的性和针对性。降低了维修费用和企业成本，提高了变电站技术管理水平和安全管理水平。

参考文献：

[1] [poly-oitcssV3.0]在线红外温度连续监测系统白皮书[M]. 2011, 11.

[2] 孙晓刚, 李云红. 红外热像仪测温技术发展综述[J]. 激光与红外, 2008, 38(2): 4-7.

[3] 钱家骊, 黄瑜珑, 徐国政. 智能化高压开关设备的开发与应用[J]. 高压开关行业通讯, 1997, (12): 33-36.

[4] 徐东晟, 许一声.高压开关柜触头温度在线监测的研究[J]. 高压电器, 2001, 37(1): 54-55.

[5] 陈衡, 侯善敬. 电力设备故障红外诊断[M]. 北京: 中国电力出版社, 1999.

[6] 田勇, 田景林. 6～10KV开关柜事故统计分析与改进意见[J].东北电力技术, 1996, (8):5-10.

[7] 杨立. 红外热像仪测温计算与误差分析[J]. 红外技术, 1991, 21(4): 20-24.

[8] 李博. 变电站主电气设备状态监测和故障诊断技术应用[J].中国电力,2002,(35):40-44.

[9] 张良胜, 张杰. 红外在线监测系统在封闭开关柜中的应用[J]. 电网技术, 2008, (32): 155-158.

【上接第25页】

中物联网管理者保障信息安全、管理好物联网有一定的借鉴意义。

参考文献：

[1] 冯登国, 张阳, 张玉清. 信息安全风险评估综述[J]. 通信学报, 2004, (07).

[2] 邓聚龙. 灰色系统基本方法[M]. 华中科技大学出版社, 2005.

[3] 罗党. 灰色决策问题分析方法[M]. 黄河水利出版社, 2005.

[4] 陈丹伟, 黄秀丽, 任勋益. 云计算及安全分析[J]. 计算机技术与发展, 2010, (02).

[5] 蒋林涛. 互联网与物联网[J], 电信工程技术与标准化, 2010, (02).

[6] 臧劲松. 物联网安全性能分析[J], 计算机安全,2010, (06).

[7] 何明, 江俊, 陈晓虎. 物联网技术及其安全性研究[J], 计算机安全, 2011, (04).

[8] 朱景锋. 基于三角模糊AHP的物联网电子政务安全评价模型分析[J]. 制造业自动化. 2012, (07).

灰色关联算法在物联网安全状态评估中的应用

作者： 高洪波， GAO Hong-bo
作者单位： 江苏城市职业学院南通校区电信系,南通,226006
刊名： 制造业自动化 ISTIC PKU
英文刊名： Manufacturing Automation
年，卷(期)： 2012,34(22)