



电信网信息内容安全事件态势感知模型研究^{*}

葛琳,季新生,江涛

(国家数字交换系统工程技术研究中心 郑州 450002)

摘要:针对电信网和信息内容安全事件的主要特征,提出了一种态势感知模型。模型通过分布式特征数据提取,采用分层递进的方式对原始数据融合后,对当前电信网络整体安全态势状况进行分析判定;针对模型的结构特点,采用基于证据理论的层次式信息融合近似算法,解决已知初始信息确定高层融合所需的概率分布的问题。仿真结果表明,该模型运算速度快、实时性好、准确度高,可以有效感知电信网络信息内容安全事件。

关键词:电信网;态势感知;证据理论;近似算法;矩阵;信度区间

doi: 10.3969/j.issn.1000-0801.2014.02.002

Research on Situation Awareness Model of Information Content Security Incidents in Telecommunication Network

Ge Lin, Ji Xinsheng, Jiang Tao

(National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China)

Abstract: Aiming at the main features of the information content security incidents and telecommunication network themselves, a design of situation awareness model was presented. The model using distributed character data collection and hierarchical progressive integration, the status of security situation of the whole telecommunication network was analyzed. According to the structure of model, hierarchical information fusion proximate calculation based on evidence theory was used to resolve the problem of how to use the initial information to determine the probability in high level information fusion. The simulation results show that the model can compute fast in real time in high accuracy, and it can perceive and determine the incidents effectively.

Key words: telecommunication network, situation awareness, evidence theory, proximate calculation, matrix, belief and plausibility interval

1 引言

电信网与互联网的融合发展,打破了传统电信网络相对封闭的格局,同时也将原本在互联网中存在的一些安全问题引入电信网^[1]。信息内容安全事件(information content security incident, ICSI)指利用信息网络发布传播危害国家安全、社会稳定和公共利益的内容的安全事件^[2]。近年来,电信网络的信息内容安全事件持续增多。以中国电信

2010年公布的统计数字为例,全网发生骚扰信息投诉量51万余次,各类安全事件均呈现快速增长势头^[3]。由此可以看出,网络IP化、终端智能化和应用多样化给各类信息内容安全事件的发生提供了便利条件,给电信网络安全带来极大的挑战。加强电信网络安全域划分,提高全网的统一安全管理能力,建设同步于电信网络发展水平的信息安全体系迫在眉睫^[4]。

网络安全监控及防护的一个重要手段就是对网络当

^{*} 国家高技术研究发展计划(“863”计划)基金资助项目(No.2011AA010605),国家科技重大专项基金资助项目(No.2012ZX03006002-010)

前的安全状况进行分析感知。态势感知技术融合可获取的信息,从宏观角度实时展现网络的整体安全态势,为网络安全管理者的决策分析提供技术依据和数据支持。目前的网络安全态势感知技术主要应用于互联网,针对电信网的研究尚处于起步阶段,而且主要针对电信网中的攻击类事件,即对网络中的病毒、操作系统漏洞、防火墙、入侵检测系统和安全日志等各防护设备所产生的数据,进行融合后做出决策评估^[5-7]。信息内容安全事件与攻击类事件相比,具有不同的特征:攻击类事件以破坏网络正常通信为目的,强度大,维度单一,通常可归为行为异常所引起的网络安全态势变化显著,较易觉察;信息内容安全事件以传播不良信息内容为目的,强度较小,多维信息,既有行为异常也有内容异常,隐蔽性大,对其所引起的态势较难把握。如何借鉴现有的态势感知技术,全方位部署电信网安全防护设备,并有效利用其产生的海量、多维安全信息做出快速、及时的融合判定,是当前电信网安全领域的研究热点。

本文基于对电信网信息内容安全事件主要特征的分析,提出一种分布式、层次化结构的态势感知模型,针对模型中数据分层融合的特点,采用基于 Dempster-Shafer(D-S)证据理论的信息融合近似算法,并在仿真环境中对模型进行了实验验证。

2 电信网信息内容安全事件特征

随着电信网和互联网融合的深入发展及多媒体业务的日益成熟,一方面,电信网所面临的信息内容安全事件形式趋于多样;另一方面,由于互联网是一个以用户为核心的非盈利性网络,很多通信业务及软件可免费使用,使得发起信息内容安全事件的成本大大降低,因此,电信网终端用户所遭受的不良信息安全事件的数量增多,同时规模变大。通过对此类事件发生时电信网络状态变化、用户通信行为和信息安全特点的研究,对其特征进行归纳,具体如下。

(1)突发性

信息内容安全事件的主要目的是通过散播非法信息内容,挑起争端、破坏社会稳定,此类事件的发生具有突发性。

(2)针对性

信息内容安全事件的目标用户通常为在特定时间段,发生了热点或敏感社会问题的区域内的用户群体,即信息内容安全事件具有一定的针对性。在这种情况下,网络中

的流量通常会有较为明显的变化趋势。

(3)干扰性

信息内容安全事件扰乱用户的正常通信,恶意占用网络资源,对于目标用户而言,接收到此类信息后,选择短时间内切断通信的用户数量较正常通信情况会有所增多,由此会引起电信网络中单位时间内,短时通话数量增多。

(4)重复性

目前,针对流量异常和短时通话数量变化等问题均已有所防护技术,而某些不良信息源为了规避检测拦截,未必会在短时间内发送大量足以引起网络流量和短时通话数量变化的信息,但其所发送的信息内容却具有相同和重复的特性。因此,对信息内容的重复性检测可作为一种有效的补充和完善。

(5)特定性

信息的传输内容通常为某种或某类特定的音/视频内容。

上述前 3 个特征可看作由用户通信行为异常引起的网络状态的变化,其中,网络流量和短时通话的变化可看作通信状态异常;后两个特征可看作通信内容异常。表 1 为信息内容安全事件的主要特征及其对电信网络通信的影响。

表 1 信息内容安全事件特征及其对电信网络通信的影响

信息内容安全事件特征		对电信网络通信的影响	当前的防护手段
突发性	针对性	流量异常	流量异常检测
	干扰性	短时通话数量增多	卡方值检测
重复性		大量信息内容重复	聚类
特定性		含有非法内容的音频	短时能量法
		含有非法内容的视频	多模态视频识别

目前业界针对信息内容安全事件的各相关特征,已经研究了相应的网络安全防护措施,但单一的安全防护措施没有综合考虑各种防护措施之间的关联性和逻辑性,无法从宏观角度掌握网络安全的需求。现代网络管理要求必须能够在动态变化的复杂环境中,对各种不确定的网管信息进行分析评估,以便网络管理员能以量化的方式,认知和理解网络中安全事件的整体状况和趋势,从而迅速、准确地做出决策。如何对各监测设备的告警数据进行分析处理,给出网络中信息内容安全事件当前的态势状况,是本文要研究的主要问题。



3 电信网态势感知模型

3.1 态势感知模型的部署

网络信息安全防护的目标是,使受保护网络中的实体和用户不受来自外部网络的攻击骚扰。也就是说,安全防护模型应处于受保护网络和外部网络之间,且假设只在它的一侧存在骚扰源^[8]。这里把受保护网络定义为可控网络(controllable network, CN), 外部网络定义为不可控网络(uncontrollable network, UN)。如图 1 所示, 假设信息源(information source, IS)为 $\{s_0, s_1, \dots, s_n\}$, 从不可控网络向可控网络实施信息攻击。骚扰方的目的是尽可能多地将不良信息传递给可控网络中的目标用户(target user, TU), $TU = \{u_0, u_1, \dots, u_m\}$ 。在可控网络的关口, 部署态势感知模型(situation awareness model, SAM)。对 SAM 而言, 其目标是能够实时感知到信息内容安全事件的发生和强度。

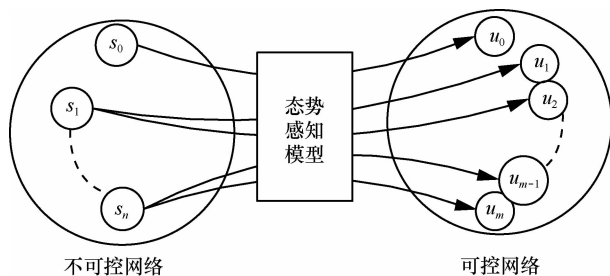


图 1 电信网信息攻击事件模型

3.2 态势感知模型的设计

SAM 实现对网络当前安全状态的感知, 首先, 需要通过数据采集获取网络中的通信数据信息; 其次, 对所获取的信息进行融合分析; 最后, 根据融合结果做出决策判定。其中, 数据采集由数据采集器(data collector, DC)完成, 信息融合(information fusion, IF)则由各级信息融合节点完成, 如图 2 所示。

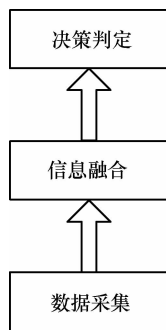


图 2 态势感知系统组成

用 $DC_1, DC_2, \dots, DC_5$ 分别表示电信网中信息内容安全事件各特征所对应的防护设备的数据采集器。数据采集器与各级融合节点 0、1、2 和 3 之间的逻辑关系如图 3 所示。 DC_1 和 DC_2 分别表示针对网络流量异常和短时通话特征的数据采集器, 当两者中有一个事件发生(即两事件为“或”的关系)时, 可认为网络中的通信状态产生异常。将其融合结果 2 与 DC_3 (内容重复性检测)再次进行融合, 判别是否有通信行为异常事件发生。 DC_4 和 DC_5 分别表示传输内容中具有特殊音频和视频特征的数据采集器, 若其中一项存在异常, 就可认为用户之间的通信内容异常, 二者即“或”的关系。

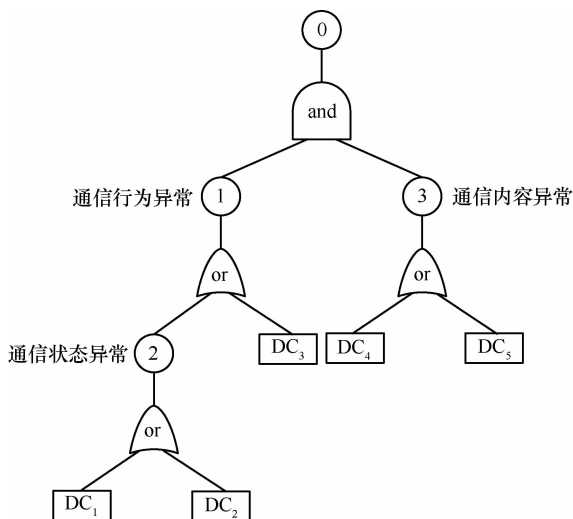


图 3 电信网络态势感知系统各节点逻辑关系

广告类信息通常发送时间集中, 发送区域有一定的特定性和内容重复性, 一般情况下也会将其归类为通信行为异常, 因此需要对具体通信内容进行识别后做出判定; 同时, 当通信内容异常时, 如果所发送的信息数量少, 则不会产生网络中流量、短时通话数量和内容重复等通信行为的异常。为了使最终融合结果更具有典型性、代表性和较强的针对性, 融合结果 1 与 3 两事件同时发生(即“与”的关系)时, 可判定当前网络中存在安全问题, 作为最终融合结果 0 输出。

通过前文的逻辑关系分析, 电信网态势感知模型可采用分布式检测, 分层、多级融合结构。模型分为数据层(data layer, DL)、信息层(information layer, IL)和知识层(knowledge layer, KL), 如图 4 所示。其中, 数据层主要由各个数据采集器完成数据信息的采集和上报; 信息层将各个数据采集器获取的信息进行初步的分类提炼和融合, 形成

对态势感知有用的信息;知识层通过数据层和信息层的数据采集、信息分类融合,形成网络当前的态势感知数据。图 4 中,局部信息融合中心(location information fusion center, LIFC)接收和处理来自多个数据采集器的信息,做出初步决策判定;系统信息融合中心(system information fusion center, SIFC)对各局部节点传送来的局部决策进行融合处理,做出系统的最终决策。

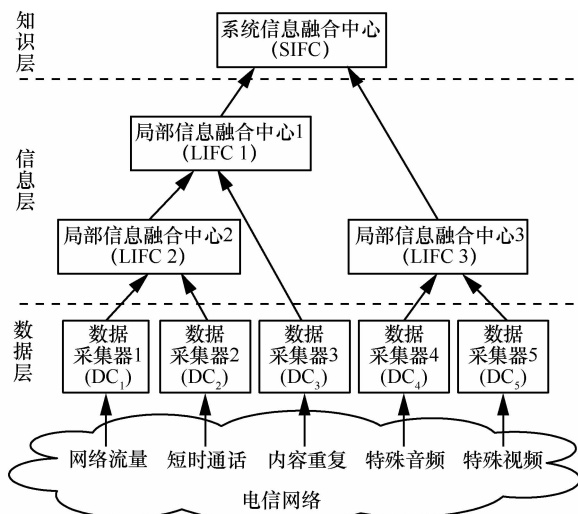


图 4 电信网络态势感知系统模型

在电信网络态势感知模型中,各个数据采集器所提供的信息一般是模糊的,包含着大量的不确定性。各级融合中心如何利用不确定性信息进行推理,从而做出正确的决策,即模型信息层融合算法的设计是整个模型能否高效运行、实现设计理念的关键。证据理论是一种重要的不确定推理方法,可以将多个不确定信息的证据进行合成,并采用区间的方法对不确定性信息进行描述,在精确反映证据聚合程度方面具有很大的灵活性。本文基于 D-S 理论,采用层次式快速信息融合近似算法,以满足电信网态势感知模型实时性和多层信息融合的需求。

3.3 模型信息层融合算法

证据理论又称 D-S 理论或信任函数理论,是对贝叶斯理论的一种扩展,其核心是证据合成准则。在证据理论中,一个样本空间称为一个辨识框架,用 $\Theta = \{H_1, H_2, \dots, H_m\}$ 表示,具有可穷性和可列性,并且其中的元素均为互斥事件。

定义 1 设 Θ 为一个识别框架,若函数 $m: 2^\Theta \rightarrow [0, 1]$ (2^Θ 为 Θ 的所有子集)满足 $m(\emptyset) = 0$, $\sum_{H \in \Theta} m(H) = 1$, 称 $m(H)$ 为 H 的基本概率分配函数或 mass 函数。

定义 2 设 $m_1, m_2, \dots, m_n$ 为识别框架 $\Theta = \{H_1, H_2, \dots, H_m\}$ 上 n 个不同的基本概率分配函数,则其正交和定义为:

$$\begin{cases} m(\emptyset) = 0 \\ m(H) = k^{-1} \sum_{\cap H_j = H} \prod_{i=1}^n m_i(H_j), H \neq \emptyset \end{cases} \quad (1)$$

其中, $k = \sum_{\cap H_j \neq \emptyset} \prod_{i=1}^n m_i(H_j)$ 。

定义 3 设 Θ 为识别框架, m 为 Θ 上的基本概率分配函数,定义函数 $Bel: 2^\Theta \rightarrow [0, 1]$ 为 Θ 上对应于 m 的信任度函数,表示对命题 H 的总的信任程度。

$$Bel(H) = \sum_{B \subset H} m(B), \forall H \subset \Theta \quad (2)$$

定义 4 设 Θ 为识别框架, m 为 Θ 上的基本概率分配函数,定义函数 $Pl: 2^\Theta \rightarrow [0, 1]$ 为 Θ 上对应于 m 的似真度函数,表示对命题 H 不否定的信任程度。

$$Pl(H) = \sum_{H \cap B \neq \emptyset} m(B) \quad (3)$$

设 $m_1, m_2, \dots, m_n$ 为识别框架 $\Theta = \{H_1, H_2, \dots, H_m\}$ 上 n 个不同的基本概率分配函数,满足:

$$\cdot 0 \leq m_i(H_j) \leq 1, \text{ 且 } \sum_{j=1}^m m_i(H_j) \leq 1, H_j \subset \Theta;$$

$$\cdot m_i(\Theta) = 1 - \sum_{j=1}^m m_i(H_j). \quad (4)$$

根据证据理论的组合规则,有:

$$m(H_j) = k^{-1} \left\{ \prod_{i=1}^n [m_i(H_j) + m_i(\Theta)] - \prod_{i=1}^n m_i(\Theta) \right\} \quad (5)$$

令 $m_i(H_j) = m_{ij}$, $m_i(\Theta) = 1 - \sum_{j=1}^m m_{ij} = t_{ij}$, 则式(5)可

以表示为:

$$\begin{aligned} m(H_j) &= k^{-1} \left[\prod_{i=1}^n \left(m_{ij} + 1 - \sum_{i=1}^n m_{ij} \right) - \prod_{i=1}^n \left(1 - \sum_{i=1}^n m_{ij} \right) \right] \\ &= k^{-1} \left(\prod_{i=1}^n y_{ij} - \prod_{i=1}^n t_{ij} \right) \end{aligned} \quad (6)$$

其中, $k = \sum_{j=1}^m \left(\prod_{i=1}^n y_{ij} - \prod_{i=1}^n t_{ij} \right) + \prod_{i=1}^n t_{ij}$ 。

将式(6)中的各因子分别用矩阵形式表示为:

$$(m_{ij})_{n \times m} = \begin{pmatrix} m_{11} & \dots & m_{1m} \\ \vdots & \ddots & \vdots \\ m_{n1} & \dots & m_{nm} \end{pmatrix}, (t_{ij})_{n \times 1} = E - \begin{pmatrix} \sum_{j=1}^m m_{1j} \\ \vdots \\ \sum_{j=1}^m m_{nj} \end{pmatrix},$$



$$(t_{ij})_{n \times m} = \begin{pmatrix} t_1 & \cdots & t_1 \\ \vdots & \ddots & \vdots \\ t_n & \cdots & t_n \end{pmatrix} \quad (7)$$

通过运算即可求得 $m(H_j)$ 、 $m(\Theta)$ 和各个状态的信度区间 $[Bel(H_j), Pl(H_j)]$ 。将融合结论转化为下一步证据融合的 BPA 为:

$$m(H_i) = \begin{cases} \frac{\sum_{A_i} V}{\sum_{i=1}^n \sum_{A_i} V} \\ \frac{\int_{e_1 \subseteq A_i} \int_{e_2 \subseteq A_i} \cdots \int_{e_n \subseteq A_i} (e_1 e_2 \cdots e_n)^a d e_1 d e_2 \cdots d e_n}{\sum_{i=1}^n \int_{e_1 \subseteq A_i} \int_{e_2 \subseteq A_i} \cdots \int_{e_n \subseteq A_i} (e_1 e_2 \cdots e_n)^a d e_1 d e_2 \cdots d e_n} \end{cases} \quad (8)$$

其中, A_i 表示第 i 个信度区间在空间形成的区域, V 表示离散数据源在 A_i 区域内的体积, $e_1, e_2, \cdots, e_n$ 表示连续数据源各个证据的正态分布函数^[9,10]。

3.4 模型的主要特点

模型的主要特点介绍如下。

- 可靠性高: 采用分布式检测方式, 利用多数据采集器对同一事件进行多层次反复融合确认, 有效降低事件的不确定性, 提高系统决策的可信度。
- 容错性强: 根据通信网络特征进行数据采集器的部署, 覆盖面广。当某些数据采集器出现故障或错误时, 系统经过适当的融合处理, 仍有可能得到正确结果。
- 实时性好: 采用分层的融合方式, 大大减少了系统和局部信息融合中心的处理数据量, 可获得实时结果。
- 决策时间短: 模型内部连接简便, 通信压力小, 数据传输及时准确, 提升了模型的决策速度。
- 准确度高: 模型充分考虑电信网信息内容安全事件的特征, 综合利用各采集器获得的特征数据, 信息量充足, 融合所得出的判决结果最为贴近实际网络状态。
- 可扩展性强: 随着网络的不断发展, 不良信息的传播手段随之增多。模型采用的分布式层次化结构只需在原有基础上, 针对新的不良信息传播手段, 增设数据采集器及局部信息融合中心即可, 升级方式简单、易行。

4 仿真实验

4.1 仿真实验环境

当前电信网信息内容安全事件手段多样, 包括音频、视频类多媒体信息。为了验证模型的有效性, 本文选取中国电信目前采用的、支持可视电话业务的 IMS 网络作为测试模板。IMS 网络的核心协议为 SIP。试验中的 SIP 终端用户设置可利用网上开源的 BOL SIP phone 软件实现, 而 SIP 网络中的重定向、媒体网关和服务器等功能则可以由单独的设备实现, 也可以与 SIP 代理集成在同一设备中实现, 灵活性大, 简单易行。基于此, 本文选择建立 SIP 网络环境, 对电信网态势感知模型进行仿真实验。

如图 5 所示, 骚扰方从受保护网络左侧向 SIP 网络中的用户发起攻击, 特征介绍如下:

- 在预置的特定时间段内, 向受保护网络中的某特定区域 A/B/C 中的用户发起攻击;
- 用户端接收到不良信息电话的挂机概率随机确定;
- 不良信息源向受保护网络中用户发送的通信信息具有重复性;
- 不良信息源向受保护网络中用户发送某特定音频内容;
- 不良信息源向受保护网络中用户发送某特定视频内容。

针对以上 5 个特征, 分别进行多次数据统计, 作为 D-S 证据理论的初始概率分布。

4.2 仿真实验结果

实际网络安全事件强度曲线如图 6 所示, 电信网态势感知模型检测的态势曲线如图 7 所示, 将两者进行对比分析, 可以看出: 随着安全事件强度的增大, 对应的网络态势感知值也随之上升; 当安全事件强度变小时, 网络态势评估值随之降低, 但网络态势感知值下降的斜率较安全事件强度下降的斜率小。这是因为, 在高层信息融合中, 使用信度区间对网络安全状况进行表述, 使得落在区间内的值都将产生不同程度的告警。这一点在实际网络环境的应用中具有重要意义, 即当某信息内容安全事件在短时间内再次发生时, 网络仍可保持一定的警戒度。

图 8 为态势感知模型预测结果与实际攻击情况曲线的对比。可以看出, 预测的结果是一条较平滑的曲线, 与实际安全事件情况基本相符。

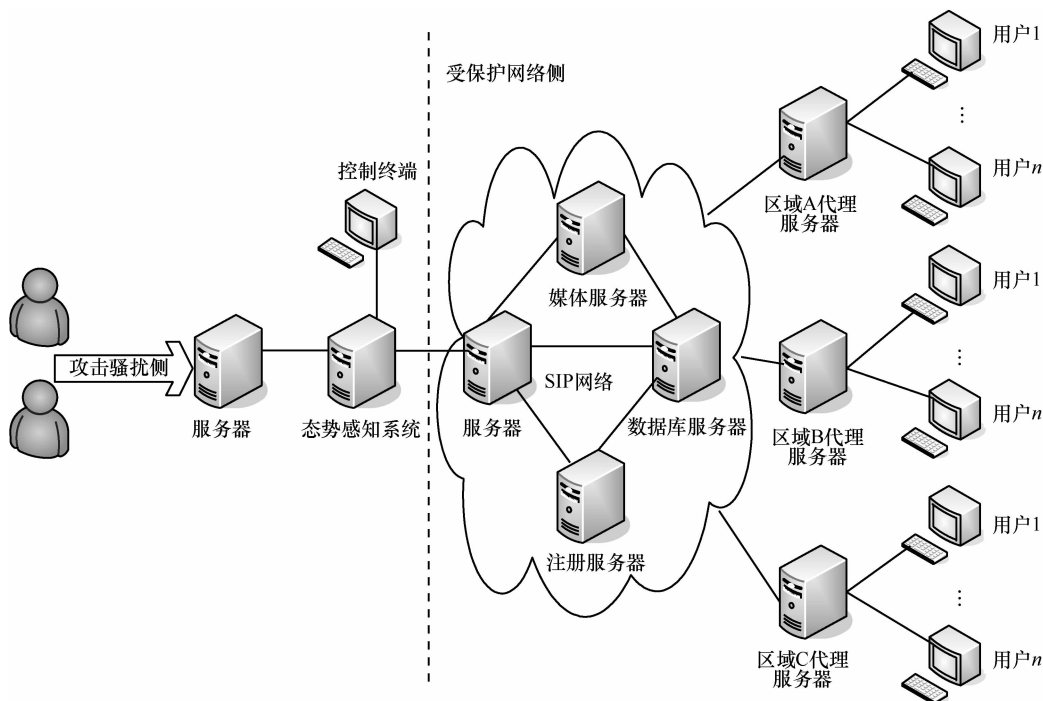


图 5 仿真实验环境搭建

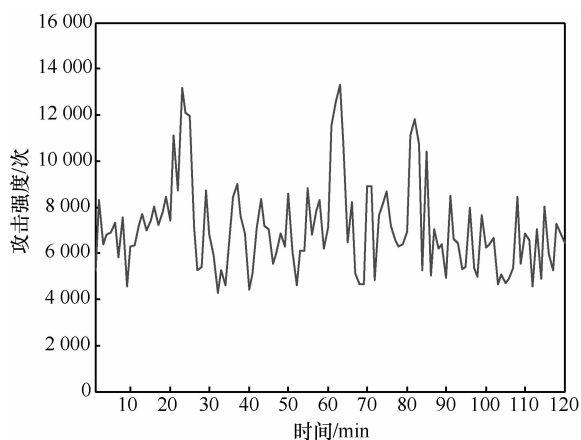


图 6 攻击强度与时间的关系

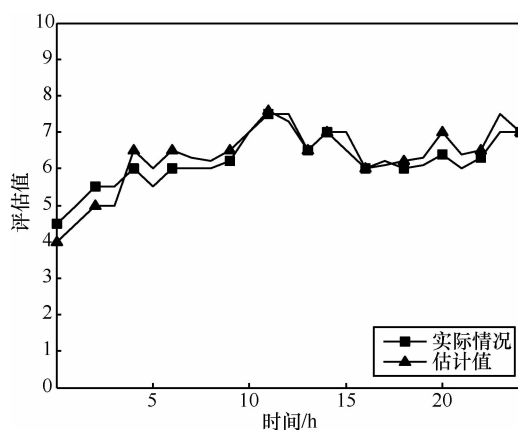


图 8 网络感知与实际情况的对比

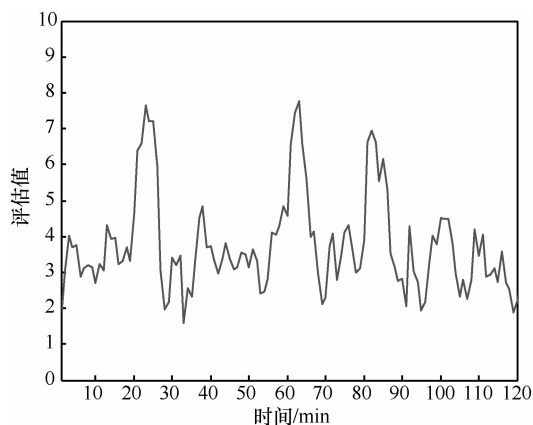


图 7 网络评估与时间的关系

实验结果表明,本文提出的电信网络态势感知模型能够把握网络安全态势的总体变化趋势,对网络安全状况做出及时感知,判定结果与实际情况接近,具有较高的准确度^[11-17]。

5 结束语

近年来,电信网络的安全问题备受关注,态势感知技术是其中的研究热点。目前电信网的态势感知技术仅针对攻击类事件,而针对信息内容安全事件态势感知的研究尚属空白。本文通过对电信网和信息内容安全事件自身特点的分析,提出了态势感知模型的设计方案。针对此模型采用的分



层结构的特点,采用了一种基于 D-S 理论的层次式信息融合近似算法,并在仿真环境中对该模型进行了实验验证。仿真结果表明,该模型可以有效感知信息内容安全事件。

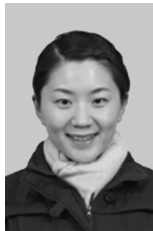
该方案为维护电信网络信息安全和用户合法权益提供了技术支持。但本文目前提出的基于 D-S 证据理论的层次式融合算法并没有考虑证据冲突的情况,虽然特征提取的针对性强,可以有效避免冲突证据的发生,但为保证算法的完整性,这点需要进一步研究和改进。同时,现有方案在仿真实验环境中可靠、有效,下一步将针对实际网络的运行环境进行实验验证。

参考文献

- 1 万晓榆,樊自甫,宗晓飞. 下一代网络安全技术. 北京: 人民邮电出版社, 2007
- 2 中国标准化管理委员会. 信息安全事件分类分级指南. GB/Z 20986-2007, 2007
- 3 中国电信集团公司. 中国电信网络安全技术白皮书, 2010
- 4 中国电信集团公司. 中国电信网络安全技术白皮书, 2011
- 5 杨肖. 下一代电信网安全态势评估系统设计. 北京邮电大学博士学位论文, 2008
- 6 卢宇. 下一代电信网风险分析系统的研究与实现. 北京邮电大学博士学位论文, 2009
- 7 林帆. 下一代网络安全态势评估系统中数据缓存子系统的设计与实现. 北京邮电大学博士学位论文, 2010
- 8 陈训逊, 方滨兴, 胡铭曾等. 一个网络信息安全的新领域——网络信息渗透检测技术. 通信学报, 2004, 25(7): 185~191
- 9 冷宣兵, 王平, 张立. 证据理论合成准则的一种新算法及其验证. 计算机仿真, 2010, 27(2): 162~165
- 10 孙锐. 基于 D-S 证据理论的信息融合及在可靠性数据处理中的应用研究. 电子科技大学博士学位论文, 2011
- 11 彭敏. 基于免疫的网络入侵检测与风险预测模型. 计算机工程, 2011, 37(11): 141~143
- 12 Holsopple J, Sudit M, Nusinov M, *et al*. Enhancing situation awareness via automated situation assessment. IEEE Communications Magazine, 2010(1): 146~152

- 13 Parvar H, Fesharaki M N, Moshiri B. Shared situation awareness system architecture for network centric environment decision making. Proceedings of Second International Conference on Computer and Network Technology, Bangkok, Thailand, 2010: 372~376
- 14 Nguyen-Thanh N, Koo I. Empirical distribution-based event detection in wireless sensor networks: an approach based on evidence theory. IEEE Sensor Journal, 2012, 12(6): 2222~2228
- 15 Zhu L, Shi D, Duan X. Evidence theory-based fake measurement identification and fault-tolerant protection in digital substations. IET Generation, Transmission & Distribution, 2011, 5(1): 119~126
- 16 Liao J, Bi Y X, Nugent C. Using the dempster-shafer theory of evidence with a revised lattice structure for activity recognition. IEEE Transactions on Information Technology in Biomedicine, 2011, 15(1): 74~82
- 17 Li Y B, Wang N. Based on D-S evidence theory of information fusion improved method. Proceedings of 2010 International Conference on Computer Application and System Modeling, Taiyuan, China, 2010: 416~419

[作者简介]



葛琳,女,国家数字交换系统工程技术研究中心博士研究生,主要研究方向为网络信息安全。

季新生,男,国家数字交换系统工程技术研究中心教授、博士生导师,主要研究方向为网络安全。

江涛,男,国家数字交换系统工程技术研究中心讲师,主要研究方向为移动互联网安全。

(收稿日期:2013-08-22)

·简讯·

2013 年 12 月电话用户分省情况

2013 年 12 月份统计数据显示,全国固定电话用户数为 26 698.5 万户,其中城市电话用户数为 18 456.8 万户,农村电话用户数为 8 241.7 万户;全国移动电话用户数为 122 911.3 万户。

全国统计的电话用户主要分布在东部、中部和西部地区。东部固定电话用户数为 14 500.2 万户,其中城市电话

用户数为 9 863.8 万户,农村电话用户数为 4 636.4 万户;东部移动电话用户数为 61 702.2 万户。中部固定电话用户数为 6 633.2 万户,其中城市电话用户数为 4 516.0 万户,农村电话用户数为 2 117.1 万户;中部移动电话用户数为 31 450.8 万户。西部固定电话用户数为 5 565.2 万户,其中城市电话用户数为 4 077.0 万户,农村电话用户数为 1 488.2 万户;西部移动电话用户数为 29 756.4 万户。

(来源:工业和信息化部运行监测协调局)