一种分布式网络情报框架的模型*

焦 健[1], 李 琦[2], 李肖坚[3]

(1. 北京信息科技大学 计算机学院, 北京 100101; 2. 中国工商银行软件开发中心, 北京 100193; 3. 广西师范大学 计算机学院, 广西 桂林 541004)

摘 要: 为解决已有的网络情报系统由于串行工作模式产生的效率和可靠性较低的问题,设计了一个分布式的网络对抗情报框架,框架使用统一的情报描述语言实现各情报子系统间的协同工作。使用 Petri 网仿真分析表明该框架具备良好的可靠性,真实环境下软件测试结果显示该框架对情报系统运行具有较好的效率支持,能够满足网络对抗的实际需要。

关键词: 网络对抗; 情报框架; 分布式系统; Petri 网

中图分类号: TP393.04 **文献标志码**: A **文章编号**: 1001-3695(2012)08-3053-03

doi:10.3969/j.issn.1001-3695.2012.08.065

Distribution computer network intelligence frame model

JIAO Jian[1], LI Qi[2], LI Xiao-jian[3]

(1. *College of Computer, Beijing Information Science Technology, Beijing* 100101, *China*; 2. *Software Development of ICBC, Beijing* 100193, *China*; 3. *College of Computer, Guangxi Normal University, Guilin Guangxi* 541004, *China*)

Abstract: In order to resolve the problem that efficiency and stability is poor, because the intelligence system mainly works on serial model. This paper proposed a distribution computer intelligence frame. This frame used consistent intelligence language for collaborative work by module. Simulation using Petri net to validate the frame show the stability is well. In the reality environment with the software of this system, the frame has well efficient to support the intelligence system, it can be satisfied with the requirement of network operation.

Key words: network operation; intelligence frame; distribution system; Petri net

计算机网络对抗由计算机网络攻击、计算机网络防御和计算机网络利用组成,旨在为获取信息优势而在计算机网络上采取增强和维护己方的信息能力、并阻止和削弱对方这种能力和努力的活动与行为[1]。

计算机网络对抗需要采用攻击、防御、利用等多种行为,有别于传统的计算机网络攻防和安全,网络对抗还需要有充分可靠的信息支持,彼此之间通过这些信息的交换完成整个对抗行为,这些信息在军事领域被统称为情报。文献[2]将情报活动划分为四个子活动构成:整合(integration)、评估(evaluation)、分析(analysis)和解释(interpretation)。这四个子活动可能顺序执行,也可能同时执行。

对于网络对抗的双方而言,其核心的内容是发现和判定网络中存在的漏洞和网络的运行态势,对抗双方分别发现、掌握对方与己方的漏洞和态势,从而制定并执行各自有针对性的方案。针对网络中的漏洞发现技术目前已经比较成熟,其中典型的应用如文献[3,4],其核心内容在于基于知识库,使用推理引擎产生相关的网络漏洞信息。但目前此类工作只是围绕特定获取的网络数据进行,当网络中的数据源呈现多样性、不确定性时,就需要有相应的数据整合、评估[5]等工作的支持,而这需要有成体系的情报系统。

针对此类问题,文献[6]最早提出了网络对抗情报系统的建立;文献[7]在此基础上提出了一种支持网络情报的模型,为整个对抗提供必要的关于网络漏洞、安全态势等情报,该模型的功能结构固定,其主要的工作方式为串行性的工作方式,虽然能够准确地为网络对抗提供信息支持,但其效率不高,同时系统模块间采用紧耦合的连接方式。

本文设计了一个网络对抗情报的框架,该框架为分布式工作方式,通过统一的接口和情报描述语言,实现系统模块间的松耦合,以框架数据库为基础,提供情报模块间的调度功能。

1 情报框架

计算机网络对抗情报框架需要解决的主要问题是实现情报系统的松耦合问题,为各个模块提供基本的信息交互的功能、情报系统的构成,从功能角度划分可以有以下几个部分:

a)整合。负责从外部将获取的信息按照信息的种类规整,作数据级的合并,一般的整合是以网络目标为基础。

b)评估。收到已经归类的信息后,对信息进行可信度评价,评估的目的主要是对未知确定源的信息给出一个可信度,便于后面的分析。

c)分析。利用已经知识库,对当前可以使用的可信数据进行加工,得到有价值信息,一般采用推理机制,实现数据到信息和知识的转换,在这一阶段情报开始生成。

d)解释。计算机网络对抗的情报和人的主观意识之间存在理解差异,解释活动完成这部分差异消除的工作。

为了将各功能模块有效地联系起来,首先需要构造模块之

收稿日期: 2011-12-22; **修回日期**: 2012-02-14 **基金项目**: 国家自然科学基金资助项目(61170295);北京市教委科技面上项目(201211232010)

作者简介:焦健(1978-),男,河北沧州人,博士,主要研究方向为计算机网络对抗(jiaojian@bistu.edu.cn);李琦(1982-),女,系统分析师,硕士,主要研究方向为网络安全、软件测试;李肖坚(1961-),男,教授,博士,主要研究方向为计算机网络安全、计算机网络对抗.

间的接口,即框架的整体结构。这些接口主要包括:

a)接口 INPUT。从外部获取数据,交给整合模块,实现外部输入到整合功能的连接。

b)接口 I1。从整合功能模块获取归类后的信息,传入存储单元。

c)接口 I2。从存储单元中读取归类的信息,传入评估接口,同时接收评估后的信息,存入存储单元。

c)接口 I3。完成框架中存储单元与分析模块的交互,实现整个情报系统的分析过程。

d)接口 I4。对分析后得到的信息交付解释模块,完成信息到情报的转换,并将转换结果返回存储单元。

f)接口 OUTPUT。存储单元的情报以外部对抗所需要的形式输出。

在确定完以上输出接口的基础上,整个框架组织情报系统按照整合→评估→分析→解释的顺序产生情报。但需要指出的是,这个过程中各个活动都存在并行的可能性,即在整个过程中框架需要具有相应的数据存储单元,因此在框架内部设置数据库系统。整个系统的交互结构如图 1 所示。

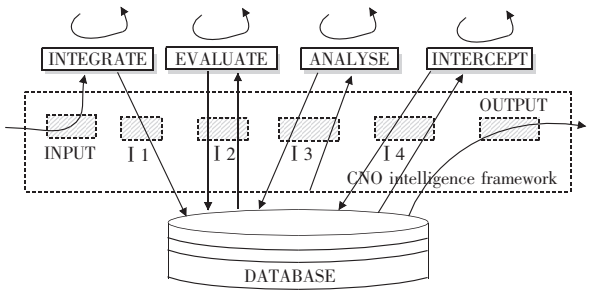

图 1 软件框架结构

为了实现以上模块的基本构成,框架系统设计了情报描述语言,用以实现各个模块之间的传输。主要包括基本数据类型定义、基本描述语句定义、信息描述语句定义、情报描述语句定义等。其中基本描述语句和情报描述语句是核心,用于表征网络中的目标态势和目标的情报态势。主要描述语句如下:

〈target〉::=target‘(’〈role〉‘,’〈location〉‘)’

〈role〉::=enemy|ours|unknown

〈location〉::=〈net〉|〈node〉|〈process〉|〈service〉|〈file〉|〈n-connect〉|〈p-connect〉|〈s-connect〉

〈net〉::=〈address〉‘/’〈mask1〉|〈address〉〈mask2〉

〈intelligence〉::=Intelligence‘=’‘(’〈date〉〈time〉〈target〉〈actuality〉〈deduction〉‘)’

其中:〈date〉、〈time〉、〈target〉、〈actuality〉、〈deduction〉分别是日期、时间、目标、现状和发展趋势的描述语句,具体定义包含于态势描述语句。

框架为各个模块提供了基本的交互语言之后,需要为每个接口提供语言解释器以完成交互,主要接口解释器包括:

a)输入语言解释器。输入情报表述,产生形式的目标现状,主要用于 INPUT。

b)整合接口解释器。产生情报数据库变量的形式,主要用于 I1。

c)评估接口解释器。实现数据库变量与评估输出之间的双向转换,主要用于 I2。

d)推理接口解释器。实现情报数据库和情报生成引擎之间的双向转换,在实现中此处使用了 Prolog 的推理语言,因此实际转换形式为情报数据库与 Prolog 之间的转换,主要用于 I3。

e)输出语言解释器。实现情报数据库变量到情报描述语言形式的转换,主要用于 I4。

为进一步分析框架系统的特性,以框架接口功能为核心,构造形式化模型。为描述方便使用 TARGET 表示目标,ACTUALITY 表示网络情况,COLLECTOR 表示收集器,VULNER 表示漏洞信息,DEDUCTION 表示推论。其中接口 OUTPUT 不做形式上的转换,其他接口涉及到的转换形式如下:

a)INPUT

$$\begin{cases} \mathrm{IN}_{\mathrm{input}} = \{t,a\} \\ \mathrm{OUT}_{\mathrm{input}} = \{(t,a)\} \end{cases}$$

b)I1

$$\begin{cases} \mathrm{IN}_{\mathrm{integration}} = \{t,a\} \\ \mathrm{OUT}_{\mathrm{integration}} = \{(t,a) \mid T(t) \in \mathrm{TARGETTYPE}\} \end{cases}$$

其中:$t \in$ TARGET,$a \in$ ACTUALITY,TARGETTYPE 是目标类型,即 $T(t)$ 表示同种类型目标的集合。

c)I2

$$\begin{cases} \mathrm{IN}_{\mathrm{evaluation}} = \{(t,a,c) \mid T(t) \in \mathrm{TARGETTYPE}\} \\ \mathrm{OUT}_{\mathrm{evaluation}} = \{(t,a,C(t,a)) \mid 0 \leqslant C(t,a) \leqslant 1\} \end{cases}$$

其中:$c \in$ COLLECTOR,$C(t,a)$ 表示目标 t 的现状 a 的可信度。

d)I3

$$\begin{cases} \mathrm{IN}_{\mathrm{analysis}} = \{(t,a) \mid C(t,a) \geqslant n, 0 < n \leqslant 1\} \\ \mathrm{OUT}_{\mathrm{analysis}} = \{(t,v)\}; \end{cases}$$

其中:$v \in$ VULNER。

e)I4

$$\begin{cases} \mathrm{IN}_{\mathrm{interpretation}} = \{(t,v)\} \\ \mathrm{OUT}_{\mathrm{interpretation}} = \{(t,d)\} \end{cases}$$

其中:$d \in$ DEDUCTION。

2 Petri 网仿真建模

针对各种接口的定义,本文使用有色 Petri 网构建系统的形式化模型。具体步骤主要包括:

a)确定系统的库所,框架系统中涉及到的库所如表 1 所示。

表 1 模型库所

place	describe	attribute
P_{in}	整合模块	外部组分
P_{ev}	评估模块	外部组分
P_{an}	分析模块	外部组分
P_{inte}	解释模块	外部组分
INPUT	框架后的数据	内部组分
DATA	整合后获得数据	内部组分
REL	评估后的数据	内部组分
INFO	生成的信息(情报)	内部组分
KNOW	解释后的知识	内部组分
OUTPUT	输出后的情报内容	内部组分

b)确定变迁元素、变迁系统主要对应解释器 a) ~ d)中的变化,其中为了区别接口和外部模块的功能,对于 I2、I3 和 I4 三个主要变迁按照框架和外部接口的进出顺序,都细化为两个子变迁,即 T' 和 T''。

c)确定令牌种类,主要包括:tar(目标)、a(现状数据)、c(收集器信息)、cta(信息来源可信度)、vul(漏洞信息)和 de(情报的解释结果)。为方便系统仿真结果的表示,令牌以组合方式出现在模型的库所中,其组合如表 2 所示。

表 2 令牌组合

令牌	含义	令牌	含义
tar × a	输入的目标和态势信息	tar × a × cta	每条信息的评估结果
tar × a	整合后存储的态势信息	tar × v	分析后生成的情报
tar × a × c	标有收集器的信息	tar × de	经过解释处理后的情报

d)构造有向弧。构造整个系统模型,给予 Petri 网的情报框架模型如图 2 所示。

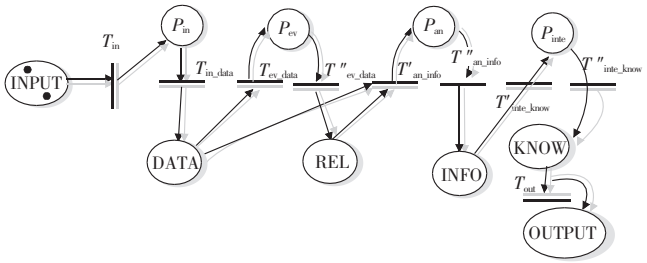

图 2　框架 Petri 网

3　系统运行与分析

为验证模型的可行性,分别采用形式化分析和系统实例运行两种手段,形式化分析主要用于分析模型的特征,实例运行则主要用于测试网络中的主机漏洞信息的生成。

首先在框架的 Petri 网模型基础上,使用 CPN-Tools 对系统的计算时空复杂度进行分析,主要包括可达性的验证和库所有界性的分析结果。

从分析结果来看,当框架外部输入的数据从 1 000 条增加到 10 000 条时,代表时间复杂度的步长增长态势如图 3 所示。从步长的增长方式来看,框架的运行时间消耗比为线性增长方式,不存在组合爆炸的问题。

框架计算的空间复杂性可以用系统的有界性衡量,输入的托肯为 100 ~ 500。从计算的结果来看,系统的各库所(表 3)中的最大上限基本保持在某一个恒定的数值或区间中。该数据表明系统在运行过程中,框架中各接口的存储数据其容量保持在一个稳定的数值,不会出现随着输入量激增而空间激增的情况。

表 3　库所空间容量上限

DATA	INTEGRATE	EVALUATE	ANALYSE	INTERCEPT
[32,34]	[33,34]	11	6	4

模型的公平性、家性、活性等性质如表 4 所示。从分析结果看,系统不存在无法发生的序列,即框架中的各个组件都会得到均等的触发。家性可以表明系统中不存在可以重新返回到任意变迁的序列,即框架中的运行状态不会产生不可预知的逆向活动。系统的活性主要通过死变迁和活变迁来进行识别。两种变迁都不存在的情况表明,框架中的接口模块不存在不会被触发的部分,同时每一个接口在没有新的输入前提下,不可能被重复触发,这也保证了整个系统运行的稳定性。

表 4　性能分析结果

公平性	家性	活变迁	死变迁
no infinite occurrence sequences	none	none	none

通过对框架的 Petri 网建模分析可以了解框架在支持情报系统并行运行时所具有的特征,以证明框架对并行系统的支持可能。另一个方面,框架对情报系统的调度运行过程中势必消耗一定的时间,需要对框架运行的时间效率问题作进一步的分析。

在 Visual Studio C ++6.0 环境下实现了该框架模型,同时利用 MySQL 数据库和 XSB 引擎实现了框架与情报模块的集成。为检验数据系统的功能,在分布式平台上利用已有的情报描述语言,该情报描述语言主要来源于 CVE[8],用于实现在指定操作系统、服务软件的情况下,产生指定的漏洞信息。框架外部的功能模块主要包括数据整合、评估、生成和解释四个部分以及输入/输出的接口部分,分别输入 1 000 ~ 10 000 条情报描述语言,各个接口所用时间和模块所用时间的比例如图 4 所示。从实验分析结果来看,输入/输出接口相对耗时最大,占整个系统的耗时 60% 以上,而整合、评估、分析和解释的主要接口的操作耗时较少。

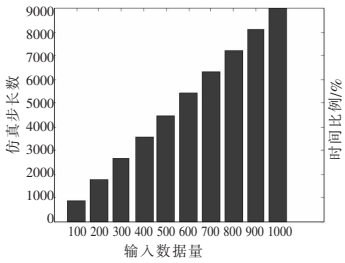

图 3　系统可达趋势

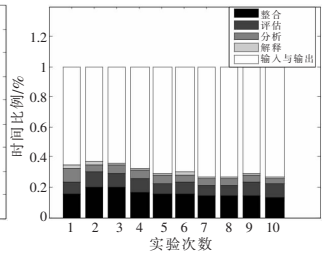

图 4　系统运行时间比例

此外,从统计时间来看,框架的内部模块最多仅占用了 0.6% 的系统运行时间,其余大约 99.4% 的系统运行时间由情报生成的功能模块(外部系统)占用。由于采用并行处理的方式,整个框架的功能集中在对接口的信息交互和数据库的访问方面,情报系统的时间消耗主要集中在分析、评估等功能模块中。由此可知,系统的情报框架高效地实现了系统中模块间的交互,具有较好的工作效率。

4　结束语

计算机网络对抗是计算网络安全发展到战略层面后的一种必然形式,除了具备传统意义上的网络攻击、防御等能力外,以获取攻防所需信息情报为目的的情报系统是整个体系正常运行的保障。为增强系统的可靠性、适应复杂多变的网络环境,本文设计实现了分布式网络情报系统的框架,提供了模块间统一情报描述语言,以及为情报系统使用的数据库系统。这些都有效地支撑了整个系统的分布式运行。本文所设计的框架,其实验数据证明该系统具有较好的效率,功能上可以有效地支持情报系统的实现,同时也实现了系统的松耦合。

框架的实现为整个情报系统的实例化提供了有力的支撑。需要指出的是,情报系统中各个功能对应复杂的网络环境,针对漏洞、网络态势的判断具有一定的模糊和随机性,如何处理这些问题,是未来的研究内容。

参考文献:

[1] Joint Chiefs of Staff. Joint publication 1-02: department of defense dictionary of military and associated terms [M]. Washington DC: Joint Publication, 2007.

[2] Joint Chiefs of Staff. Joint publication 2-01: joint and national intelligence support to military operations [M]. Washington DC: Joint Publication, 2004.

[3] Nmap free security scanner[EB/OL]. (2008-10-11)[2011-12-12]. http://www.insecure.org/nmap.

[4] ANDERSON H. Introduction to nessus[EB/OL]. (2007-01-05)[2011-12-12]. http://www.securityfocus.com.

[5] SUN Yun-yun, YAO Shan, LI Xiao-jian, *et al*. An evaluation model of CNO intelligence information confidence[C]//Lecture Notes in Computer Science, Vol 5854. Berlin: Springer, 2009: 400-412.

[6] 李肖坚. 一种计算机网络自组织的系统对抗模型[J]. 计算机研究与发展, 2005, 42(A): 618-628.

[7] 姚珊. 基于对等通信的计算机网络对抗战术情报系统研究与实现[D]. 北京: 北京航空航天大学, 2007.

[8] CVE version: 20061101 CVE Candidates as of 20111206 [EB/OL]. (2006-11-01)[2011-12-12]. http://cve.mitre.org/cve/cve.html.