学校编码：10384　　分类号_____密级_____
学号：X2013230489　　UDC ____

厦门大学

工 程 硕 士 学 位 论 文

面向公安网络的智能运维监控系统的设计与实现

Design and Implementation of Intelligent Monitoring and Maintenance System for the Public Security Network

鲁 潜

指 导 教 师 ：林坤辉 教授
专 业 名 称 ：软 件 工 程

论文提交日期：2015 年 3 月
论文答辩时间：2015 年 4 月
学位授予日期：2015 年 月

指 导 教 师：_____
答辩委员会主席：_____

2015 年 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明,并符合法律规范和《厦门大学研究生学术活动规范(试行)》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

随着公安信息化建设的不断推进，公安部门信息系统的应用水平有了很大的提高。信息化水平的提升带来了减本增效、方便快捷，然而整个信息系统的复杂度也不断增加。目前，国际信息安全形势日趋尖锐，IT 技术的发展和普及使得内网泄密的风险大大增加。在这种背景下，公安网络的信息化运维管理人员面临的不仅仅是信息系统的运行维护问题，而是信息系统运维与网络安全的有机结合，运维人员应当形成一种综合全面的网络安全运维监控机制，确保信息系统的可用性，确保各种安全保密规章制度能够切实得到落实，从而确保信息系统的可用性与安全性。

本文研究了面向公安网络智能运维监控系统的研究与实现问题，深入分析了信息系统可用性和安全性评价指标，包括：基础性能、网络性能、网络运行参数、服务与进程状态以及操作系统与补丁状态；接着研究了对这些指标进行监控的方法；然后对系统的框架和各个模块进行设计，最后进行了开发与实现。

本文从网络设备、网络拓扑和主机三个方向入手，分别研究了它们各自的的性能指标、数据采集方式和数据比对方法。对于网络设备而言，它的网络性能、路由表、ARP、VLAN 表、IP 地址表和网络拓扑是监控的重点，因为它们反映了网络系统的运行状态；对于主机而言，服务器的基础性能、服务器与进程情况、操作系统与补丁情况则需要重点进行关注。另外，本文提出了一种对网络业务自动进行运维的方案，能够大大降低网络管理员的工作负担。对于所有的指标，均讨论了在 SNMP 和 WMI 这两种技术下进行实现的可行性。

基于以上研究，本文设计实现了一个面向公安网络智能运维监控系统。整个系统基于.NET 进行开发，采用模块化分层设计，具有良好的移植性和扩展性。

关键词：公安网络；运维；监控

Abstract

With the development of public security information technology, application level public security departments of information systems has been greatly improved. This has reduced the cost and increased efficiency and brought a lot of convenience, but the complexity of the entire information system is also increasing. At present, the international information security situation is becoming increasingly acute, the development and popularization of the IT technology has greatly increased the risk of leaks.In this context, public security information system managers are facing not only the operation and maintenance issues but also the network security issues. They should form a comprehensive network security operation and maintenance monitoring mechanism to ensure the availability of information systems, to ensure that all security rules and regulations can be implemented effectively, thereby ensuring the availability and security of information systems.

In this dissertation, the research and implementation issues the public security network oriented intelligence operation and maintenance and monitoring system, in-depth analysis of the information system availability and security are embodied by which indicators, and how to monitor these indicators, this critical issue, then the system framework and each module are designed, and finally the system is developmented and implemented.

This dissertation starts from the network devices , network topology and hosts , investigated their respective performance indicators, data collection methods and data comparison methods. For network devices, its network performance, routing tables, ARP, Vlan table, IP address and network topology is the focus of the monitoring, because they reflect the operational status of the network system; for the host, server performance basis, services and processes status, the operating system and patches are need to focus on. In addition, this dissertation presents a network operation and maintenance automated business solutions, can greatly reduce the workload of network administrators. All of the indicators are discussed in SNMP and WMI about the feasibility to achieve.

Based on these studies, the dissertation designed and implemented a public security network oriented intelligence operation and maintenance and monitoring system.The whole system is based on .NET environment, adopting a modular hierarchical design with portability

and scalability.

Key words: Public Security Network;Operation and Maintenance; Monitoring

目录

第一章 绪论 1

1.1 研究背景 1

1.1.1 网络安全运维研究现状 1

1.1.2 网络安全运维应用现状 2

1.2 本文内容 4

1.3 本文结构 4

第二章 相关技术介绍 5

2.1 SNMP 协议 5

2.2 WMI 组件 7

2.3 拓扑发现 11

2.4 本章小结 13

第三章 系统需求分析 14

3.1 系统业务需求概述 14

3.2 系统功能需求分析 15

3.2.1 数据采集功能需求分析 15

3.2.2 数据处理功能需求分析 20

3.2.3 告警管理功能需求分析 21

3.2.4 网络运维功能需求分析 21

3.2.5 配置管理功能需求分析 22

3.3 本章小结 23

第四章 系统设计 24

4.1 系统设计原则 24

4.2 系统框架设计 24

4.3 数据采集模块设计 25

4.4 数据处理模块设计 39
4.5 告警管理模块设计 42
4.6 网络运维模块设计 43
4.7 配置管理模块设计 46
4.8 本章小结 50
第五章 系统实现 51
5.1 开发环境 51
5.2 系统实现 52
5.2.1 数据采集与处理 52
5.2.2 告警管理模块 55
5.2.3 网络运维模块 56
5.2.4 配置管理模块 59
5.3 本章小结 60
第六章 总结与展望 61
6.1 总结 61
6.2 展望 61
参考文献 62
致谢 64

CONTENTS

Chapter 1 Introduction 1

1.1 Research Background 1

1.1.1 Relevant Researches of the Network Security Operation and Maintenance Issues ... 1

1.1.2 Relevant Appliances of the Network Security Operation and Maintenance Issues ... 2

1.2 The Main Contents 4

1.3 Structure 4

Chapter 2 Related Technology Introduction 5

2.1 SNMP 5

2.2 WMI 7

2.3 Topology Discovery 11

2.4 Summary 13

Chapter 3 System Requirements Analysis 14

3.1 System Business Requirements Dscription 14

3.2 System Functional Requirements 15

3.2.1 Data Acquisition Requirements 15

3.2.2 Data Processing Requirements 20

3.2.3 Alarm Management Requirements 21

3.2.4 Network Operation and Maintenance Requirements 21

3.2.5 System Configuration Requirements 22

3.3 Summary 23

Chapter 4 System Design 24

4.1 System Design Principle 24

4.2 System Frame Design 24

4.3 Data Acquisition Module Design 25

4.4 Data Processing Module Design 39

4.5 Alarm Management Module Design 42

4.6 Network Operation and Maintenance Module Design 43

4.7 System Configuration Module Design 46

4.8 Summary 50

Chapter 5 System Implementation 51

5.1 Implementation Environment 51

5.2 System Implementation 52

5.2.1 Data Acquisition and Processing 52

5.2.2 Alarm Management 55

5.2.3 Network Operation and Maintenance 56

5.2.4 System Configuration 59

5.3 Summary 60

Chapter 6 Conclusions and Prospect 61

6.1 Conclusions 61

6.2 Prospect 61

References 62

Acknowledgements 64

第一章 绪论

1.1 研究背景

随着信息化建设的不断推进，公安机关信息系统的应用水平有了很大的提高。信息系统增强了公安干警侦察破案、远程协作、行政管理的能力，使得工作效率和工作质量极大提高。随着日常的办公、办案电子化、网络化的不断推进，信息系统的规模和复杂程度直线上升。在享受信息化带来的减本增效、方便快捷的同时，面向公安网络的信息系统运维管理问题也成为当下的一个重要课题。

目前，国际信息安全形势日趋尖锐，部分发达国家依托其科技的不对称优势建立了规模庞大的网络空间侦查体系，部分 IT 巨头、知名设备商都有参与。根据媒体报道，国外情报机构通过这些手段窃取了大量的机密信息。与此同时，网络安全问题已经引起各国的普遍重视，我国已经成立了中央网络安全和信息化领导小组。网络侦查窃密与信息安全防护之间的对抗正在升级。

当前，计算机网络在技术发展和普及覆盖方面有了长足的进步，具体表现为[1]：1.网络规模正在不断扩大；2.有线网、无线网、蜂窝网以及物联网络等开始互联，网络接入日趋复杂；3.移动互联网方兴未艾，已经覆盖到了社会的边边角角；4.网络带宽不断提升，千兆局域网已经成为主流，基于 LTE 的 4G 通信已经投入应用，移动通信也拥有了高速的网络接入。然而对于信息系统运维管理人员来说，负面的效应就是内网信息泄密的途径和风险大大增加了。

1.1.1 网络安全运维研究现状

国外从上个世纪 80 年代中期就开始对网络运维管理的技术进行完整、系统的分析和研究。其中，以 IEEE、ISO、ITU-T 等组织为主体的研究机构主要致力于网络安全管理框架、结构和标准的制定和开发，并取得了卓著的成果这些标准的确立大大地推动了网络安全运维管理的行业发展。

目前，被广大网络安全运维技术专业人员所熟知的网络管理标准是 SNMP，事实上它已经成为了业界标准。许多 IT 巨头都已 SNMP 为基础开发了商业产品，比如 HP 公司的 OpenView、IBM 公司的 Tivoli NetView、Nortel 公司的 Java Device Manager、BMC 公司的 Remedy、Cisco 公司的 CiscoWorks、优利普华的 UNIPER 以及 Zoho 公司的 ManageEngine OpManager 等[2]。此外，优秀的开源产品也在不断涌现，常见的包括

Centron 系统、OpenNMS 系统、OMD 系统、Icinga 系统、Nagios 系统、Zenoss 系统以及 NagVis 系统等。然而，这些国外开发的网络运维管理系统存在一些共性问题：与本土的管理应用模式存在一定的偏差而且价格昂贵。有的系统只能在厂商自家的设备上运行，兼容性较差。目前，在国内商业市场上也有许多同类产品，如联软科技的 LeagView、北塔的 BTNM、摩卡的 Mocha BSM、广通的 BroadView、神州泰岳的 Ultra、华为的 iManager、锐捷的 RG-SNC-Pro、中兴的 NetNumen、汉远网智的 sonic 等等，都在国内占据了一定的市场份额。这些产品各有侧重点，共同的特点是针对性太强，功能不够全面，只能涵盖网络运维管理全周期的部分环节。在这种状况下，许多单位不得不采取这样的网络运维管理模式：选择一个扩展性较好的系统作为基础平台，然后根据需要拿其它针对性较强的系统进行功能性叠加。通过这种拼凑来形成较为广泛和全面的网络安全运维监管体系。然而其中的不足也很明显，那就是各个监管环节之间没有进行有效的整合和联动，使得整体的效果不尽人意。

长久以来，网络安全与网络运维相互独立，很少混为一谈。网络技术的快速发展和网络攻防技术的不断涌现推动着网络安全市场也在不断成长，相关成果也很多。具体的产品主要以硬件为主，如防火墙、IDS、IPS、堡垒机、网络安全审计系统等。启明星辰、绿盟、天融信等国内厂商都有较为全面的产品线，基本能够满足企业网络安全的需求。然而由于网络安全问题自身的特殊性，国外的产品在国内的竞争中天然处于劣势。

总的来说，目前网络运维产品与网络安全产品是相互独立的，暂未看到将对于网络安全运维问题的综合解决方案。因此，网络运维管理不得不继续采用系统拼凑的方式来解决信息系统的可用性和安全性问题。

1.1.2 网络安全运维应用现状

在当今的时代背景下，在较大规模和复杂度的网络中，现有的网络安全运维管理模式存在着诸多问题，主要有以下几点：

1. 网络运维与网络安全分而治之

信息系统管理人员仍然将网络运维问题与网络安全问题分开考虑，忽视了其中的关联性。实际上，科学严格的运维管理是能够提升整体的网络安全性的。

2. 对信息系统运行状态的监测不够全面

信息系统运行状态包含的内容非常多，比如网络拓扑分布、设备的基本运行情况、接口与流量情况、路由表等反映网络整体运行状态的信息。设备基础性能又包含了内存

的占用率、CPU 的占用率等。受限于各家厂商对于标准的支持情况不同，现有的网络运维管理产品基本都无法对以上全部信息进行全面兼容和覆盖。

3. 对网络拓扑结构的监测不够深入

用户私自在网络中接入交换机等网络设备，或者将室内交换机转移接入位置，都会造成网络拓扑发生变化。这些未授权的行为可能会绕过网络安全体系的监测和限制，存在巨大的安全隐患。现有的网络运维管理软件基本都能做到对于网络拓扑结构的发现，然而对网络拓扑的改变进行监测的还不多。

4. 未对终端进行有效的监控管理

现有的网络运维管理的重点工作基本都放在服务器、交换机等设备上，而忽略了终端的重要性。诚然，终端的宕机、掉线并不会影响整个信息系统的可用性，然而从网络安全的角度来说，所有的终端都是内网的边界节点，它们的安全防护水平可能决定了整个信息系统的最低防护水平，任何一个终端被外部攻破都可能导致内网信息的泄露。而且，与服务器、交换机等设备不同的是，终端都是分散管理的，它的运行状态、接入行为都存在着一定的不可控风险，更加容易成为信息系统整体防护网的漏洞。部分单位目前已经意识到了这一点，制定了相应的制度对主机非法接入网络、私自更换主机部件、安装违规软件等行为进行禁止，然而并没有一种强力的检查监督手段，在管理过程中比较被动。

5. 运维自动化水平不高

目前的网络运维管理软件的基本都将自己的角色定位为运维人员与设备之间的接口，传达运维人员的操作，并返回设备的状态。运维人员的工作虽然从纸质化变成了电子化，但仍然是全手动的操作模式，并没有从日常的简单重复劳动中解放出来。 甚至在某些方面，运维人员仍然在一大堆纸质的表格档案中苦苦耕耘。

从以上问题可以看出，目前的网络安全运维管理解决方案大多没有从信息安全的角度来考虑信息系统的运维管理事务，网络运维也没有给网络安全带来多少提升。实际上，网络管理系统可分为可用性、安全性和管理型三个层次。可用性是网络系统运行的最低要求，其次是安全性。这两个层次的实现依赖于准确实施的网络监测，对当前网络的运行状态进行智能的分析，以便于及时发现已经发生或将要发生的故障和隐患，自动排除故障或为运维管理人员给出有效可行的故障排除建议或方案，保证故障能够迅速得以排除。网络系统的配置、计费等等属于更高层次的需求，它属于日常运维管理的范畴，它的目的是使网络系统保持一种健康、高效、易于管理的状态。

1.2 本文内容

本文研究面向公安网络的智能运维监控系统的关键技术与实现方法。首先研究了相关的技术：SNMP、WMI 以及一种数据链路层网络拓扑发现算法。然而从提升公安内网可用性和安全性的目的出发，分析了系统的业务需求和功能需求。接着，设计了系统的框架结构和各个模块的业务逻辑，涵盖了节点性能、网络拓扑、安全性、网络业务自动运维等关键问题。接着对系统进行了开发实现。最后，总结本文成果，并展望了下一步的研究与开发工作。本文的主要工作如下：

1. 分析介绍了一种高效的、能够探测哑设备的数据链路层网络拓扑发现算法以及网络拓扑比对方法；

2. 分析了公安网络在可用性和安全性方面存在的问题和需求；

3. 研究了内网节点性能、网络拓扑、安全性的监测与告警方法，以及网络业务自动运维的实现技术；

4. 对系统进行需求分析、设计并开发实现。

1.3 本文结构

本文的结构组织如下：

第一章：介绍本文的研究背景,包括网络安全运维管理的研究和应用现状，分析现有方案存在的不足，提出本文要解决的主要问题，介绍本文的章节安排；

第二章：介绍网络安全运维监控的相关技术；

第三章：从业务、功能的角度对系统进行需求分析；

第四章：对系统的整体架构和各个模块的业务逻辑进行设计；

第五章：选择开发环境，进行系统的开发实现；

第六章：对本文的工作进行梳理和总结；分析了本系统的不足之处，展望了下一步系统需要完善的地方、下一步的研究方向和需要注意的底层技术。

第二章 相关技术介绍

目前可以见到的网络运维管理解决方案基本都是以 SNMP 和 WMI 为技术基础。经过多年发展，它们已经趋于成熟并得到广泛应用。网络拓扑发现是网络管理中的重要问题，本文也将对它的相关技术进行介绍和分析。

2.1 SNMP 协议

SNMP 诞生于 1988 年，它的设计目标是解决基于 TCP/IP 协议簇的网络系统的管理问题。根据当时的计划，SNMP 只是一个临时性的网络管理框架，它是公共管理信息协议(Common Management Information Service, CMIP)成熟并普及前的一个替代性方案，因此它功能简单而又非常的稳健。SNMP 推出后得到了广泛的应用和支持，主要是因为它在简单性、灵活性和扩展性等方面达到了理想的平衡。目前 SNMP 已经成为了网络监控管理方面的事实标准[错误!未定义书签。][3]。

SNMP 工作模型是基于代理(Agent)构建的。代理是运行在被管设备上的管理组件。在正常情况下，网络管理站向代理查询或设置相关信息，代理进行消息反馈；在异常状况下，代理也可主动进行报告。SNMP 工作模型如图 2.1 所示。

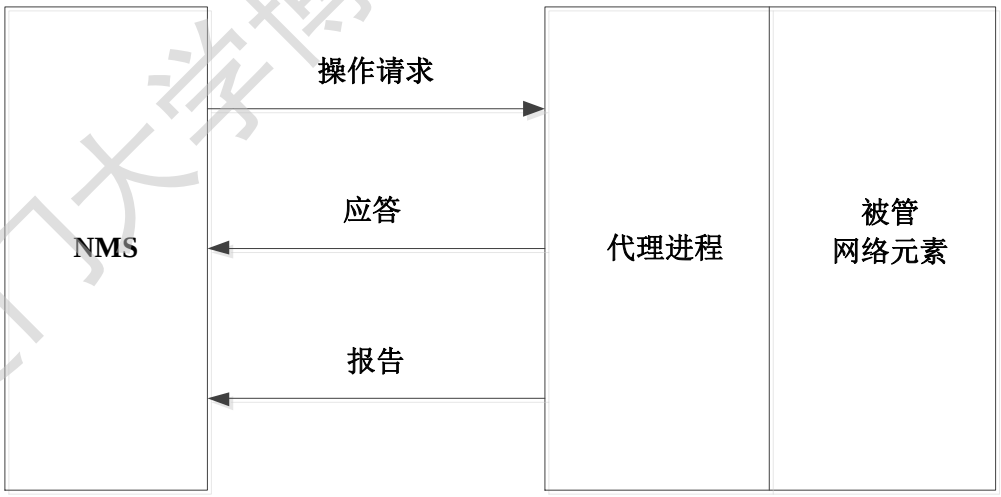

图 2.1 SNMP 的工作模型

SNMP 工作在应用层，使用 UDP 协议。默认情况下，网络管理站将请求发送到被管设备的 161 端口；被管设备则将 Trap 发送到网络管理站的 162 端口。SNMPv1 规定了 5 种操作，分别对应着一种 PDU[4]，如表 2.1 所示。

表 2.1 SNMPv1 中的 PDU 分类

PDU 代码	PDU 类型	说明
0	GetRequest	管理者发出的查询请求，PDU 中指明了要求查询的对象。被管设备使用 GetResponse 返回请求的数据。
1	SetRequest	管理者发出的设置请求，PDU 中指明了要求设置的对象。被管设备使用 GetResponse 返回 set 结果。
2	GetNextRequest	管理者发出的查询请求，查询的对象为 PDU 中指明的对象的下一个。被管设备使用 GetResponse 返回请求的数据。
3	GetResponse	被管设备发出的应答，其中包含了请求的数据、处理结果和错误信息。
4	Trap	被管设备发出的报告，用于报告本设备发生的异常事件。

SNMP PDU 封装格式如图 2.2 所示。

图 2.2 SNMPv1 的 PDU 格式

图 2.2 中上部分为前四种 PDU 结构，下部分为 Trap PDU 的结构，它们略有不同。请求标识符(request ID)是由管理进程设置的一个整数值，用于标识网络管理站的请求。网络管理站常常会同时向许多代理发出许多请求，而先发送的请求有可能反馈的更晚，因此代理进程在发送响应报文时也要返回此请求标识符，这样才能够将响应报文与请求报文对应起来。

UDP 是不可靠的传输协议，然而 SNMP 体系并没有采取任何确保可靠性的机制，因为设计者认为重传和确认会浪费网络资源并增加复杂性[5]。因此，实际应用中的可靠性需由应用程序自行解决。比如，如果在一定时间内没有收到应答则认为请求已经丢失，