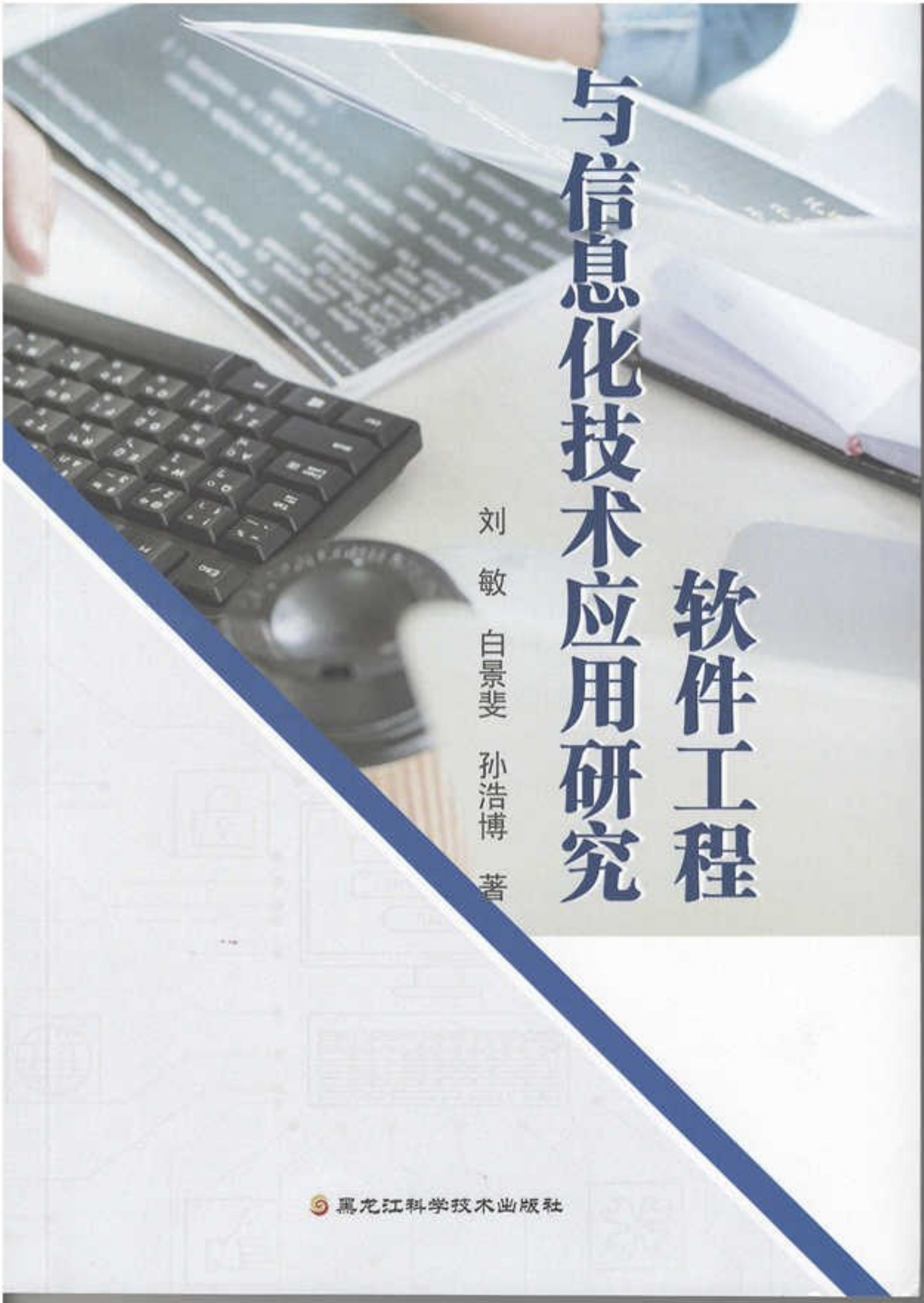


软件工程与信息化技术应用研究

刘敏 白景斐 孙浩博 著

黑龙江科学技术出版社

图书在版编目（CIP）数据

软件工程与信息化技术应用研究 / 刘敏, 白景斐, 孙浩博著. — 哈尔滨 : 黑龙江科学技术出版社, 2021.9
ISBN 978-7-5719-1098-3

Ⅰ. ①软… Ⅱ. ①刘… ②白… ③孙… Ⅲ. ①软件工程—研究②信息技术—研究 Ⅳ. ①TP311②G202

中国版本图书馆CIP数据核字(2021)第177869号

软件工程与信息化技术应用研究
RUANJIAN GONGCHENG YU XINXIHUA JISHU YINGYONG YANJIU

作　　者　刘　敏　白景斐　孙浩博
责任编辑　郑　毅
封面设计　刘梦杳
出　　版　黑龙江科学技术出版社
地　　址　哈尔滨市南岗区公安街70-2号　邮编：150001
电　　话　（0451）53642106　传真：（0451）53642143
网　　址　www.lkcbs.cn　www.lkpub.cn
发　　行　全国新华书店
印　　刷　廊坊市瀚源印刷有限公司
开　　本　710 mm × 1000 mm　1/16
印　　张　20.125
字　　数　310千字
版　　次　2021年9月第1版
印　　次　2021年9月第1次印刷
书　　号　ISBN 978-7-5719-1098-3

定　　价　50.00元
【版权所有，请勿翻印、转载】

随着我国经济的
发展迅速。软件工程
有效的、实用的和高
言，数据库，软件开
面。在现代社会中，
电子邮件，嵌入式系
译器，数据库，游戏
的应用，比如工业，
用促进了经济和社会
提高了生活质量。

信息化是以现
研究对象各要素汇
习、辅助决策等和
术，使用该技术后，
低成本。信息技术的
量的提高，人们的
户可知天下事，人不
在教学上的应用，
灵活，教育方式个
络，自觉或不自觉地
购物、远程医疗、

本书共十一章
中心）负责第一章
白景斐（山西电力
撰写，计10万字；
公司）负责第九章
晓丽（宁夏财经职
万字。

前言

随着我国经济的飞速发展，计算机软硬件技术、信息技术发展迅速。软件工程专业是一门研究用工程化方法构建和维护有效的、实用的和高质量的软件的学科。它涉及到程序设计语言，数据库，软件开发工具，系统平台，标准，设计模式等方面。在现代社会中，软件应用于多个方面。典型的软件比如有电子邮件，嵌入式系统，人机界面，办公套件，操作系统，编译器，数据库，游戏等。同时，各个行业几乎都有计算机软件的应用，比如工业，农业，银行，航空，政府部门等。这些应用促进了经济和社会的发展，使得人们的工作更加高效，同时提高了生活质量。

信息化是以现代通信、网络、数据库技术为基础，对所研究对象各要素汇总至数据库，供特定人群生活、工作、学习、辅助决策等和人类息息相关的各种行为相结合的一种技术，使用该技术后，可以极大的提高各种行为的效率，并且降低成本。信息技术的广泛应用促进了人们的工作效率和生活质量的提高，人们的工作方式和学习方式也正发生转变，足不出户可知天下事，人不离家照样能办事。网络技术，多媒体技术在教学上的应用，使得人们的学习内容更丰富，学习方式更灵活，教育方式个性化、远程化。人们将广泛地利用信息网络，自觉或不自觉地使日常生活便捷化，如：居家上班、网上购物、远程医疗、网上交友等。

本书共十一章，其中第一作者刘敏（济南市不动产登记中心）负责第一章至第三章内容撰写，计10万字；第二作者白景斐（山西电力职业技术学院）负责第五章至第八章内容撰写，计10万字；第三作者孙浩博（青岛新闻网络传播有限公司）负责第九章至第十一章内容撰写，计8万字；副主编解晓丽（宁夏财经职业技术学院）负责第四章内容撰写，计3万字。

ISSN 1001-7119

全国中文核心期刊　　中国科技核心期刊

科技通報

BULLETIN OF SCIENCE AND TECHNOLOGY

2017年11月第33卷 第11期
Vol.33 No.11 Nov. 2017

浙江省科学技术协会主办
Sponsored by Zhejiang Association for Science and Technology

ISSN 1001-7119

中国·杭州
HANGZHOU CHINA

·交通运输·

·环境科学·

·教育、科学·

期刊基本参数:CN33-1079/N*1985*12*16*280*zh*P*￥10.00*1250*63*2017-11

基于G-K算法的网络安全态势预测模型

白景斐[1],赵文仓[2]
(1.山西电力职业技术学院,太原 030025;2.青岛科技大学 自动化学院,青岛 266042)

摘 要:针对普通Kalman算法在网络安全态势预测中对初始数据的依赖性较高,且预测精度不够高的问题,本文提出了一种基于G-K算法的网络安全态势预测模型。首先利用灰关联熵分析方法选出影响网络安全态势的关键因素,然后结合关键因素建立网络安全态势的多元关系模型,最后选用KDD-cup99的部分数据作为实验数据源对改进算法进行实例仿真。结果表明,G-K算法能够快速跟踪网络安全态势的变化趋势,预测精度优于普通Kalman算法。

关键词:G-K算法;网络安全;态势预测;屋面优化;灰关联熵分析;关键因素分析

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1001-7119(2017)11-0216-04
DOI:10.13774/j.cnki.kjtb.2017.11.050

Network Security Situation Prediction Model Based on G-K Algorithm

Bai Jingfei[1], *Zhao Wencang*[2]
(1.Shanxi Electric Power Vocational and Technical College, Taiyuan 030025, China;
2.Qingdao University of Science and Technology, Qingdao 266042, China)

Abstract: Aiming at the problem that the general Kalman algorithm has high dependency on the initial data in the network security situation prediction and the prediction accuracy is not high enough, this paper proposes a network security situation prediction model based on G-K algorithm. Firstly, the gray relational entropy method is used to select the key factors which affect the network security situation, and then the multivariate relation model of the network security situation is established with the key factors. Finally, some data of KDDcup99 are used as the experimental data source to simulate the improved algorithm. The results show that the G-K algorithm can quickly track the trend of network security situation, and the prediction accuracy is better than that of ordinary Kalman algorithm.

Keywords: G-K algorithm; network security; situation prediction; roof optimization; gray relational entropy analysis; key factor analysis

对网络的安全态势进行研究,探究其未来发展的方向,就可以更好而又更加全面地把控网络安全态势[1]。要想对网络安全态势进行预测,就需要了解过去和现今的网络状态,通过对比,就可以对网络安全进行推断[2]。评估网络安全的过程中,需要达到的最为重要的结果就是预测网络安全态势,这也是最为重要的一个环节[3]。例如灰色关联模型或者贝叶斯模型都是最为传统的对网络安全进行预测的方法,在统计学中相对有较多的使用者[4]。传统的统计学模型尽管无法对网络的终极目标进行判定,但能够基本反馈出网络安全的基本状态[5]。比如前文讲到的灰色关联模型,虽然无法保证对数据进行精准的预测,但是能够较为清晰地反馈出网络态势的发展情况[6]。由于网络安全监测的重要性,相当多的专家学者针对预测网络安全态势进行研究和分析,也确实发现了很多问题,主要问题存在于时间序列方面,专家在验证的过程中,发现造成问题最

收稿日期:2016-12-06
作者简介:白景斐(1983-),女,汉族,山西太原,研究生学历,计算机应用,E-mail:bjf61853@163.com。

为主要的原因在网络式非线性的状态特征,但是运用的统计学方法呈现出线性特征[7]。这样就无法通过传统算法对网络安全态势进行预测,需要加入一定的人工智能算法予以补助,主要会涉及到马尔可夫、神经网络、向量机(SVM)等人工智能算法,通过人工加上传统的算法,可以保证网络安全态势的预测有更加精准的范围[8]。马尔可夫、神经网络、向量机(SVM)等人工智能算法也存在如下弊端:在对SVM参数进行选择的过程中,会具有较强的盲目性,受到选择者的个人主观意识比较强烈,由于没有理论作为依据进而导致样本数据进一步增加,会让算法的进程十分缓慢;无法确定神经网络的参数,选择过程十分痛苦[9];对于马尔可夫算法而言,主要的难点在于建模的过程和繁琐公式的推导两个方面[10]。

标准Kalman算法在对网络的安全态势进行预测的过程中,存在很多问题,需要进行改进和创新,因此本文在G-K算法的基础上,构建出一个能够符合当下操作的网络安全态势预测模型,通过对该模型进行仿真实验验证,得到该算法具有有效性的结论。

1　基于网络安全态势影响因素的G-K算法

考虑到传统算法Kalman的不足,本文对灰关联熵的分析方法进行引入和学习,并在此基础上创建Grey Relation Entropy Kalman预测算法,下面简称G-K算法。G-K算法就是对传统的Kalman预测模型进行改进和创新,这样不仅仅可以动态地对网络安全态势进行分析,还能够将其不利影响降到最低,保证预测有一定的精准度。

按照如下步骤对G-K算法的预测模型进行构建:

(1)通过构建过程方程,对状态量进行描述:

$$X(k+1)=F(k)\cdot X(k)+W_1(k) \tag{1}$$

在式(1)中,状态转移矩阵用 $F(k)$ 来代表;状态在转移的过程中会有噪声产生,用 $W_1(k)$ 来代表;网络安全态势会受到 m 个影响因素的影响,用 $x_1(k)...x_m(k)$ 来代表;在某一个离散时刻 k,系统的网络安全态势值用 $x_0(k)$ 来代表;在某一个离散时刻 k 系统的状态向量用 $X(k)$ 来代表,其中 $X(k)=[x_0(k)x_1(k)...x_m(k)]^{\prime}$。

(2)通过构建观测方程,对观测向量进行描述:

$$y(k+1)=A(k)\cdot X(k+1)+W_2(k) \tag{2}$$

在上式中,某一个动态的系统时间 k 的观测向量用 $y(k)$ 来代表;观测的噪声向量用 $W_2(k)$ 代表;观测矩阵用 $A(k)$ 来代表。

2　基于G-K算法的网络安全态势预测模型

2.1　基于G-K算法的网络安全态势预测原理

(1)网络安全态势的Kalman算法

通过描述状态方程和观测方程就可以对网络安全的态势进行预测,这是因为传统的Kalman算法可以对一些离散的过程进行控制。

1)状态方程

$$X(k+1)=F(k+1,k)\cdot X(k)+W_1(k) \tag{3}$$

在式(3)中,不同的字母代表不同的含义,其中 $F(k+1,k)$ 表示的含义是从 k 时刻到 $k+1$ 时刻,系统的状态向量转移;$W_1(k)$ 表示的含义是状态转移矩阵;$X(k)$ 表示的含义是时刻 k 系统的动态状态向量。

2)观测方程

$$y(k+1)=A(k)\cdot X(k+1)+W_2(k) \tag{4}$$

在式(4)中,$W_2(k)$ 表示的含义是时刻 k 的观测噪声;$y(k+1)$ 表示的含义是时刻 $k+1$ 系统的观测向量;$A(k)$ 表示的含义是观察向量,其主要含义就是可进行观测的描述向量。

在传统的Kalman算法思想上,构建预测网络安全态势的原理,主要会受到一些关键因素的限制。如果 $k\geqslant 1$ 时,就可以求得状态向量 $X(i)$,假设 $i>n$,这样获得 n 时刻的下一段的状态量,通过描述状态量,就可以得到下一个时间的数据。

(2)新息方法

找到一个和原过程没有关系,但是具有一定的Hilbert空间特征的方法就是新息方法。$N(k)$ 表示的含义是时刻 k 的新息,从而可以运用式(5)获得网络安全态势 $y(k)$ 的全过程。

$$N(k)=y(k)-y_1(k),k=1,2,... \tag{5}$$

$y_1(k)$ 表示的含义是运用最小二乘法得出的估计值,同时也代表 $y(k)$ 的估计值。

通常而言,新息方法表现以下特性:

（1）k 时刻时，之前的数据 $y(1),y(2),...,y(k)$ 正交于新息 $N(k)$ 的数据。

（2）$\{N(1),N(2),...,N(k)\}$ 新息过程相互正交。

（3）$\{N(1),N(2),...,N(k)\}$ 新息过程的向量一一对应于 $\{y(1),y(2),...,y(k)\}$ 观测数据。

通过上述三个特性，可以知道时刻 k 之前观测数据 $y(1),y(2),...,y(k)$ 无关于时刻 k 的新息 $N(k)$，也就表明原过程与新息过程没有任何关联。新息过程是一个随机的过程，通过最小二乘法，能够得到最为准确的信息值 $y(k)$。

2.2 基于G-K算法的网络安全态势预测流程

本文的思路就是通过选择影响网络安全态势的因素，在灰关联熵分析方法之上，结合关键因素，创建多维的网络模型。下述方法为G-K算法的步骤：

Step1 设定：$y(k+1)$ 表示的含义是时刻 k 的下一个时间的网络安全态势值；$x_i(k+1)$ 表示的含义是时刻 k 的下一个时间的因素 i 的值；$y(k)$ 表示的含义是时刻 k 的网络安全态势值；$x_i(i=1,2,...,m)$ 表示的含义是 m 个根据需求选择的关键因素。以此构建回归方程，涉及到态势和关键因素两个变量：

$$\begin{cases} y(k+1)=a_{00}y(k)+a_{01}x_1(k)+...+a_{0m}x_m(k)+\partial_0 \\ x_1(k+1)=a_{10}y(k)+a_{11}x_1(k)+...+a_{1m}x_m(k)+\partial_1 \\ ... \\ x_m(k+1)=a_{m0}y(k)+a_{m1}x_1(k)+...+a_{mm}x_m(k)+\partial_m \end{cases} \tag{6}$$

在式（6）中，回归系数用两个参数 $a_{00},a_{01},...,a_{mm}$，$\partial_0,\partial_1,...,\partial_m$ 表示，可以通过最小二乘法计算得到。

$$\begin{bmatrix} \partial_0\partial_1...\partial_m \\ a_{00}a_{10}...a_{m0} \\ a_{01}a_{11}...a_{m1} \\ ... \\ a_{0m}a_{1m}...a_{mm} \end{bmatrix} = \left[T^{'}\cdot T\right]^{-1}T^{'}\cdot \begin{bmatrix} y(2)x_1(2)x_2(2)...x_m(2) \\ y(3)x_1(3)x_2(3)...x_m(3) \\ ... \\ y(n)x_1(n)x_2(n)...x_m(n) \end{bmatrix} \tag{7}$$

在上式中

$$T=\begin{bmatrix} 1 & y(1) & x_1(1)...x_m(1) \\ 1 & y(2) & x_1(2)...x_m(2) \\ ... & ... & ... \\ 1 & y(n-1) & x_1(n-1)...x_m(n-1) \end{bmatrix} \tag{8}$$

Step2 通过式（6），可以得到观测和过程方程如（9）所示：

$$\begin{cases} X(k+1)=F(k)\cdot X(k)+W_1(k) \\ y(k+1)=A(k)\cdot X(k+1)+W_2(k) \end{cases} \tag{9}$$

在上式中，$X(k)=\left[y(k)x_1(k)...x_m(k)\right]$ 表示的含义是状态向量；$F(k)$ 表示的含义是状态转移矩阵；$A(k)$ 表示的含义是观察矩阵；$W_1(k)$ 表示的含义是模型噪声；$W_2(k)$ 表示的含义是时刻 k 的测量噪音；$Q(k)$ 表示的含义是模型噪声的协方差矩阵。如果白色噪声的均值为零，那么就用 $R(k)$ 表示协方差矩阵。

Step3 初始化操作 $p(0)$ 以及 $X(0)$；

Step4 式（10）表示 $y(k)$ 这个网络安全态势的新息过程：

$$N(k)=y(k)-A(k)F(k)X_1(k-1) \tag{10}$$

$y(k)$ 的最小二乘用 $A(k)F(k)X_1(k-1)$ 表示；以此更正预测值。

根据不同 $k=1,2,3,...$ 进行推算：

$$p(k|k-1)=F(k)p(k-1)F^{'}(k)+Q(k-1) \tag{11}$$

$$kg(k)=p(k|k-1)A^{'}(k)\left[A(k)p(k|k-1)A^{'}(k)+R(k)\right]^{-1} \tag{12}$$

$$N(k)=y(k)-A(k)F(k)X_1(k-1) \tag{13}$$

$$X_1(k)=F(k)X_1(k-1)-kg(k)N(k) \tag{14}$$

$$p(k)=\left[I-kg(k)A(k)\right]p(k|k-1) \tag{15}$$

在上面的式子中，X 对应的协方差用 p 表示；Kalman增益系数用 kg 表示。在循环结束之后，运用 $y(k)=A(k-1)\cdot X(k)$ 可以计算网络安全态势值。

3 网络安全态势预测仿真

为了验证本文的G-K算法是否具有有效性，采用如下实验进行验证。首先选择具有相同配置的三台主机，其主要存在于omnet++中；其次，通过检测算法，能够得到数据源，通过对比KDD-cup99中的一些数据，就可以对相关问题进行探讨。在实验的过程中，不能够运用服务器，从而攻击smurf与land的端口，针对Perl、guess_passwd以及nmap而言，需要运用漏洞扫描进行攻击；最后运用虚拟的攻击服务器，就可以设置Perl、guess_passwd以及nmap的权重和危险性系数，分别将其设定为0.6、0.8、0.3和0.8、0.6、0.3。

在配置好实验环境后，就可以运用本文的G-K算法对网络安全态势进行预测，对于不同的结果为了更加便捷地进行分析，主要采用归一化处理。归一化处理如式（16）所示，本文的网络安全

势值范围在0到1之间：

$$x_i = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{16}$$

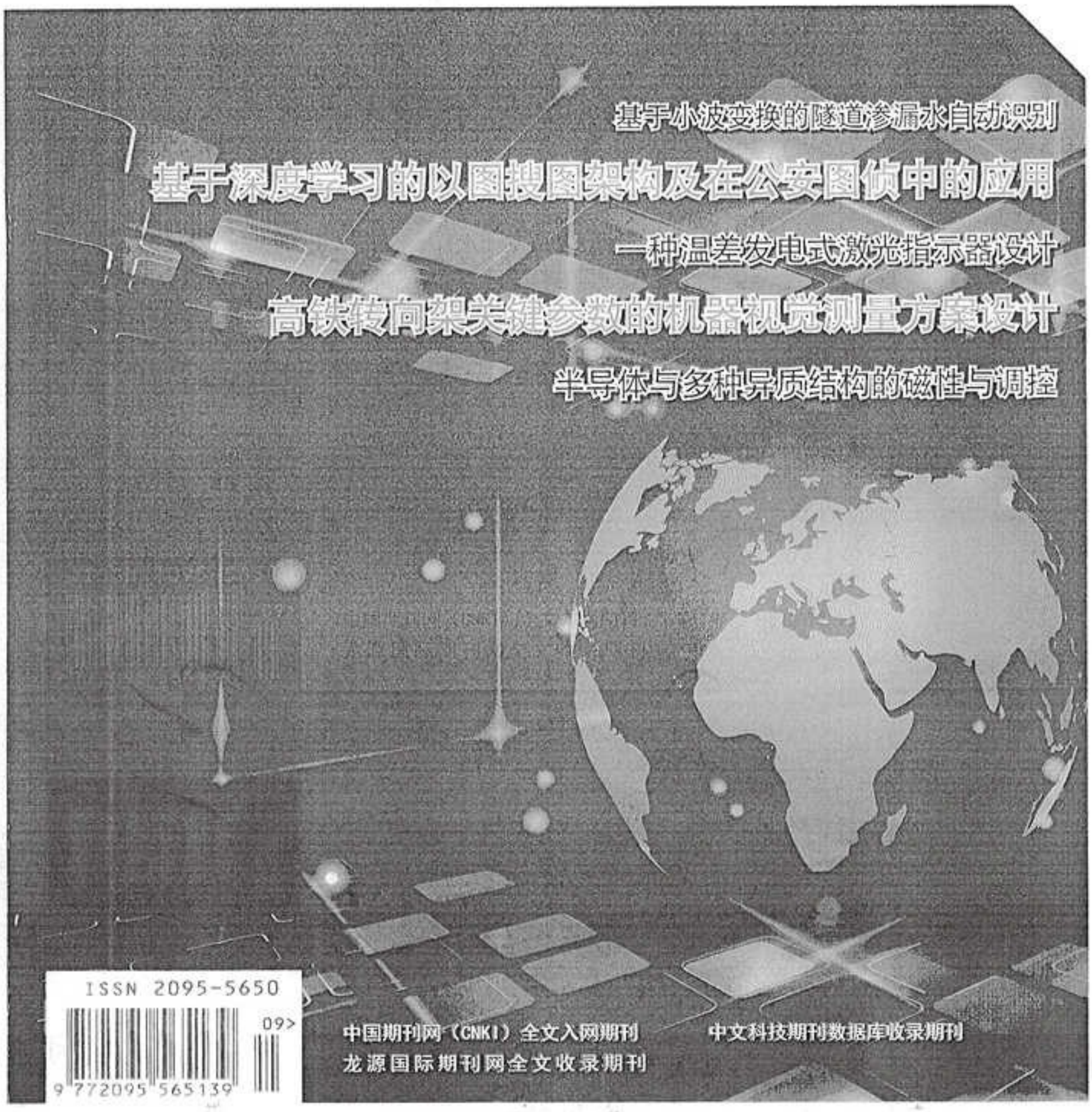
现对上式中的各个变量所代表的含义进行

主管单位:中国科学技术协会　主办单位:中国电子学会　中电新一代（北京）信息技术研究院

电子技术与软件工程

ELECTRONIC TECHNOLOGY & SOFTWARE ENGINEERING

ISSN2095-5650
CN10-1108/TP
总第131期
05
上半月刊
2018年



ISSN 2095-5650
09>
9 772095 565139
中国期刊网（CNKI）全文入网期刊
龙源国际期刊网全文收录期刊
中文科技期刊数据库收录期刊

电子信息工程中的计算机网络技术

文/[illegible]

摘要　一直以来，电子信息工程一直被人们广泛应用。但是，随着科技的发展，传统的电子信息工程已经无法满足人们的需求。现在人们日常生活所使用的电子信息产品以及[illegible]工业领域所使用的电子信息产品都是与计算机网络技术相互融合的电子信息产品。因此，本文从电子信息工程的角度阐述了计算机网络技术的[illegible]优势，包括计算机网络技术在提高信息传递速度以及提高信息安全等方面发挥的作用。

【关键词】电子信息工程　计算机网络技术　应用

随着我国人民生活水平的提高以及综合国力的提升，我们的生活与电子信息工程越来越密切。不论是工业领域、国防领域还是人们的日常生活，都离不开电子产品，离不开电子信息工程。但是科技一直在进步，现有的电子信息工程设备的信息存储功能以及信息处理功能已经不能满足我们的需求。计算机网络的出现弥补了现有的电子信息工程技术的技术缺陷，使得信息的传输速度加快，也使得电子信息工程更加安全可靠。因此，本文主要讨论了电子信息工程中的计算机网络技术的应用现状以及应用前景。

1 什么是电子信息工程中的计算机网络技术

电子信息工程是一个较为广泛的定义，电子信息工程包括所有的电子设备，包括我们日常生活中经常使用的手机、电脑、平板以及电视机等，此外电子信息工程还包括工业领域所使用的一些机器设备例如数控机床等。电子信息工程除了包括具体的电子设备，还包括一些信息处理的技术以及手段，包括信息收集技术、信息处理技术以及信息共享技术以及通信技术等。电子信息工程包括的范围较为广泛，涉及到几乎所有的信息设备以及信息处理技术，是一个综合性的概念。计算机网络技术是一种先进的信息处理设备，能够实现信息的快速传递以及共享，极大地提高了信息的传输速度，改变了人们的生活，是信息处理领域的一次重大改革。而计算机网络技术在电子信息工程中的一种信息处理技术，但是随着时代的发展，计算机网络技术目前是电子信息工程中的一项重要的技术，并在很大程度上推动了电子信息技术的发展。因此，目前人们对电子信息工程中的计算机网络技术[illegible]，[illegible]，使得信息的[illegible]，[illegible]电子信息工程的设备开发进程，是电子信息工程中一次重要的革命。

2 计算机网络技术在电子信息工程中发挥的重要作用

2.1 实现了信息的共享以及快速传递

传统的电子信息工程基本只是适用于数据的处理以及存储，在信息的传递以及共享方面并不[illegible]。因此，电子信息工程只适用于简单的信息处理，以及较为简单的数据处理。但是随着时代的发展，信息的高度共享以及快速传递成为[illegible]。计算机网络引入电子信息工程之后，电子信息工程发挥了前所未有的重要作用，不仅促进了我国国防事业的发展，促进了我国工业的发展，提高了我国的经济发展速度，还极大地丰富了人们的生活，使地球村成为现实。而计算机网络技术的先进性还体现在信息的整合方面。[illegible]。因此，计算机网络技术不仅要能够存储大量信息，还要能在短时间内传输大量信息。其次，由于信息来源复杂、分类不清，[illegible]。因此，计算机网络技术[illegible]，使得信息的共享成为现实。

2.2 大大提高了电子信息工程的安全性

[illegible]，电子信息工程的发展实现了信息的快速传递、大量传递，与此同时，对于一些不可外漏的信息，例如一些商业秘密以及[illegible]和技术等，就遭受到一定的威胁。[illegible]一旦攻入信息设备，就会泄露重要信息，[illegible]。如果信息的安全性能不能得到保障就非常不利于电子信息工程的发展，同时也会对我国经济的发展[illegible]。而计算机网络技术中，就包括一些特殊的信息技术能够保护网络安全，防止[illegible]的入侵，使得信息的安全性能得到保障。其中包括内网保护以及外网保护两种，[illegible]网络安全维护的屏障，使得重要信息以及个人信息得到有效的保护。计算机网络技术不仅能够防止病毒的入侵还能防止黑客的入侵。信息安全是信息大量传递、高度共享的基础，只有信息的安全得到保障，用户才能使用信息传输设备传递信息。

2.3 使得电子信息工程的设备开发越来越完善

信息的传输和信息处理与电子信息工程中的电子信息设备密切相关，信息的处理[illegible]需要通过设备来实现。因此，在电子设备的开发过程中，计算机网络的发展模式与计算机网络的运行模式都有很大的关系。由于计算机网络不断发展，技术不断革新，使得信息的传输效率越来越高，信息传输方式也越来越简单，电子信息的处理设备也发生了转变，电子信息工程的设备向着轻巧、高能、功能丰富的方向不断发展。另一方面，计算机网络技术解决了电子信息工程设备所存在的一系列问题，例如，解决了一些政府以及高校信息传输量过大的问题，提高了信息传递的效率以及信息的安全性能，使得信息得以平稳传递。解决了电子信息工程中通信干线所存在的线路复杂、维护工作繁琐的问题。除此之外，计算机网络技术还能提升电子信息处理设备的性能，例如在一家大型的论文共享网络中，计算机网络的[illegible]技术对论文信息实现了全球的信息传输，大大方便了人们的科学技术交流。

2.4 优化了电子信息工程的信息接收以及信息处理系统

<< 下转 11 页

2018年 6
第19卷·第6

信息记录材料

INFORMATION RECORDING MATERIALS

ISSN 1009-5624 CN 13-1295/TQ 主管：全国磁性记录材料信息站 主办：全国磁性记录材料信

中国知网全文收录期刊
万方数据库收录期刊
维普资讯网收录期刊
中国核心期刊（遴选）数据库收录期刊
中国数字化期刊数据库全文收录期刊

ISSN 1009-5624
06>
9 771009 562189
http://www.xxjlclzzs.com

新形势下我国信息网络安全问题及对策探究

庞亚萍
（山西电力职业技术学院 山西 太原 030021）

【摘要】从上世纪90年代初，计算机技术的迅速发展为信息网络提供了生存的土壤，信息网络在社会、经等诸多领域发挥着重要作用。人们通过网络实现通信和通信工具，具有良好的开放性和方便性，可节省大量时间成本，但同时也应该意识到，涉及信息安全领域，已成为一个迫切需要解决的问题。

【关键词】信息安全；网络安全；现状；对策
【中图分类号】F49 【文献标识码】A 【文章编号】1009-5624（2018）06-009

1 引言

随着云计算、移动互联网和大数据等新技术的广泛应用，信息技术已经渗透到社会生活的方方面面，成为人们生活中不可缺少的一部分。特别是新一代移动通信技术的大规模应用，使用户能够更灵活方便地进入网络，而且到处都是现实。但移动互联网和大数据技术的更新使人们在享受便利的同时，伴随而来的是一种巨大的网络信息安全的风险。对此我们国家也专门成立了中央网络安全和信息化领导小组。随着中国的崛起我们国家在国际社会上的地位在逐步提高，那么网络安全和信息化对中国的各项发展都产生着很深重的影响，在2015年7月全社会宣布“中华人民共和国网络安全法（草案）”，表明中国应该更加关注网络安全。各项政府工作报告中也对网络安全的维护做上了重要标记，但由于美国为首的西方发达国家在信息技术和产业领域占据优势，我们网络空间的安全形势更加严峻。

2 我国信息网络安全现状及面临的挑战

2.1 新一代网络关键基础设施的依赖性日益加深

在过去的十年中，随着互联网的快速发展，各行业和互联网的快速变化的商业、物流、教育中的应用，机械制造，基于许多行业中的社会生活的其他行业都建立在互联网之上的，互联网信息已经成为社会生活息息相关的内容。互联网最初的概念和原型概念源于美国。无论是网络协议地址管理还是重要的资源管理，它基本上都在美国的控制之下。例如，13个根域名服务器在世界各地的9来自美国，美国还拥有世界上最大的网络带宽，海底光缆技术的数量，最先进最；谷歌、脸谱网、推特，YouTube和一系列的全球影响力的网站，占信息服务绝对的竞争优势；美国拥有最先进的技术，在操作系统，芯片、通信设备等核心硬件和软件；Cisco、Juniper、微软、甲骨文、IBM等全球占据了大部分的市场份额等。这些资源，使世界各地的信息系统必须依靠我国的建设，对重点基础设施建设深化的依赖程度，导致安全隐患不容忽视，审查和更新完善我国现有的网络基础设施，建设高科技、高智能、强大的安全模型，新一代互联网基础设施和现代信息网络安全的发展追在后腿。

2.2 信息网络安全监管难度加大

随着互联网的快速发展，更多的人已经把互联网作为自己日常生活所离不开的设备，信息量的加大，信息传播率的速度加快都使得互联网监管的难度大大增加，再由于网络信息安全领域的环境日益复杂，互联网信息加深已经成为世界各国的重要战略目标之一，世在逐渐建立自己专门的网络信息安全管理机制，国国家安全政策委员会和美国国家安全局信息保员会的建立；美国在2009建立了国家网络安全网络安全运营中心在德国；俄罗斯设立国家信息会，对国内网络安全工作的统一部署。这样看来对于网络信息安全的重视必然会在整个全球形成的影响力，作为发展中国家的我们虽然在网络安理上也成立了专门的领导小组，但由于我们国家信息安全管理缺乏有效的协调，主要表现在相关力度不够，监管的范围不够大，影响不够深，政立管理水平较低，低效率，难度大，影响大的国络安全管理效率是很难达到风险控制的水平的，国的信息网络安全管理机制的不够完善，对于专人权整体技术的不达标，或者是技术人员的缺失，得互联网信息安全监管的难度增加，并且会随着术的发展，信息量的增大难度会越来越大。还有一点就是我们国家关于互联网网络信息的监管法够完善，中国互联网缺乏相关法规的制约，法律强有力的武器，美国不利用好，执行好，那么对于信息安全监管的难度会越来越大。

2.3 新技术的应用带来的信息网络安全威胁更多样

随着互联网的发展和进步，相关技术的衍生品虽然使人们的生活更加便利，但享受便利的也同时进一步的威胁着网络安全。例如新一代的移动通（3G、4G）的大型商业信息网络，发展全覆盖、实征更加明显，使互联网的信息更加多样性，传播速前更加快。不单单是互联网技术我们每个人都成为的信息传播渠道，那么伴随而来的就是一系列的网输出的漏洞，以及黑客，病毒的出现，严重打击了互联网的使用信心。然而新技术的应用也会使得更黑技术对我们个人的信息安全造成巨大的冲击，给全监测和预警事件带来很大障碍，政府采取措施保网络安全面临巨大挑战。

3 加强中国信息网络安全的对策和建议

3.1 加强对信息网络核心技术集成创新的支持

对于加强互联网信息安全的监管力度，我们国家在成立专门的领导小组之时，好好选拔和利用更有专