网电空间中基于 IFTS 预测模型的 IDS 方法

邢瑞康 李成海 范晓诗

(空军工程大学防空反导学院 西安 710051)

摘 要 网电空间是在信息化发展条件下随着世界军事的重大变革而产生的新兴作战空间,尤其是在防空反导对抗方面具有十分重要的影响。由于安全机制不尽完善,网络空间所要面对的威胁也不断增多。基于此背景,文中提出一种基于 IFTS 预测模型的入侵检测方法,该方法通过计算网络数据各特征属性的直觉模糊来预测误差,并通过直觉模糊预测误差来区分正常数据和入侵攻击,从而达到检测预警的目的。在此基础上,建立了入侵检测框架,并通过搭建仿真实验模拟平台来模拟一个抽象的、简化的网电空间对抗模型,对算法的有效性及效能进行验证。实验结果表明,该方法是一种有效的方法,并且在一定程度上提高了模型的检测率。

关键词 入侵检测,模糊集,网电空间,直觉模糊时间序列

中图法分类号 TP301.6 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.025

Intrusion Detection Method Based on Intuitionistic Fuzzy Time Series Forecasting Model in Cyberspace

XING Rui-kang LI Cheng-hai FAN Xiao-shi

(College of Air and Missile Defense, Air Force Engineering University, Xi'an 710051, China)

Abstract The cyberspace is an emerging combat space that has emerged under the conditions of informatization development with the major changes in the world's military, and has a particularly important impact on air defense and anti-missile confrontation. Due to the imperfect security mechanism, the threats that cyberspace faces are constantly increasing. Based on this background, this paper proposed an intrusion detection method based on the intuitionistic fuzzy time series forecasting model. This methods calculates the intuitionistic fuzzy prediction error of each characteristic attribute of network data, and distinguishes normal data from intrusion attacks by intuitionistic fuzzy prediction error, so as to achieve the purpose of detection and early warning. Based on this, an intrusion detection framework is established, and a simulation simulation experiment platform is set up to simulate the effectiveness and effectiveness of the algorithm by simulating an abstract and simplified network cyberspace confrontation model. The experimental results show that this method is effective and improves the detection rate of model to some extent.

Keywords Intrusion detection, Fuzzy sets, Cyberspace, IFTS

1 引言

当今世界正全面迈进信息化的崭新时代,而信息化时代的核心即为网络。随着网络与信息技术的飞速发展以及军事领域中空天一体化战略的深入推进,世界军事昂首迈入"信息化空天"时代,网络空间蕴藏的巨大力量以及网络资源的战略性意义正逐渐被人们发掘。随着网络的变革,世界各国在军事领域也在不断发生变化,一个全新的军事竞争平台——网电空间,成为现代军事化战争的又一主战场,并被迅速应用于陆、海、空(临空)、天各种领域。网电空间(Cyberspace)是在信息化发展条件下随着世界军事的重大变革而产生的新兴作战空间,尤其是在防空反导对抗方面具有十分重要的影响。2006 年,美参联会《联合网电作战计划》和《国家网电空间作战军事战略》将其定义为:"网电空间是借助于一定的网络环境以及相应的基础设施,利用电子和电磁频谱对数据进行存储、修改和交换的领域"[1]。然而,由于安全机制不尽完善,网络空间所面对的威胁不断增多,空天威胁也逐步成为国家安全系统面临的最为严峻的挑战。因此,对防空武器系统而言,与网电攻击对抗相关的技术研究显得十分迫切且必要。而网电空间对抗的主要目的是阻止非安全信息系统所产生的入侵行为发挥效用,因而及时发现非法入侵是网电空间系统防御体系的重要环节。

2 网电空间系统与 IDS

网电空间对抗系统中,非法入侵所实施的形式众多,通常将打击破坏敌方网络系统的作战效能作为行动目标,其作战方式具有高隐蔽性、高效性、隐性化等特性。而网电空间系统所面临的安全威胁,实质上是以网电攻击为中心的多手段的

到稿日期:2017-11-20 返修日期:2018-02-08 本文受国家自然科学基金(61703426)资助。

邢瑞康(1994—),男,硕士生,主要研究方向为网络信息安全,E-mail:18149236069@163.com;**李成海**(1966—),男,教授,硕士生导师,主要研究方向为网络信息安全等,E-mail:lichenghai2015@163.com(通信作者);**范晓诗**(1988—),男,博士,主要研究方向为网络信息安全。

综合运用和整体作用，是建立在网络系统上的作战指挥单元、武器单元的综合作用与威胁。

网电攻击的通用过程包括侦察技术和纵深防御技术，它们共同构成防空体系对抗网电攻击的基础。侦查技术主要包括对电磁信号的分类、分辨、定位与分析，对网络拓扑结构及端口主机的识别与监视，对网络流量的分析以及对网络安全态势的评估等；纵深防御技术包括信息加密技术、网络隔离技术、身份认证技术、主动防御技术等，构建起了网电空间系统安全防御体系的纵深防线。二者在网电空间系统的网电对抗技术体系中至关重要、不可或缺，是建设整个防空网电对抗体系的关键技术环节[2]。

由于任何网络攻击都难以实质性隐藏其所引起的网络数据流异常的问题，因此需要找到一种合适的异常入侵检测方法来检测和发现网络入侵的异常行为，通过合理的识别和判断对网络入侵行为进行拦截和处理。本文正是结合了上文所述的网电空间系统中网电攻击的特点，来对入侵检测技术进行研究。

3　入侵检测系统

3.1　入侵检测的原理及构成

入侵检测基于入侵行为与系统行为不同这一假设，是一种动态的网络安全技术，它通过分析网络流量或系统审计记录等，实时发现网络或系统中是否有违反安全策略的攻击行为，对可能危害到系统机密性、完整性和可用性的行为进行响应和拦截[3]。入侵的行为特征值的选择和提取是建立完整的入侵检测系统的基础，要求从网络数据报文中提取出的入侵特征值更加完备、准确和简洁。

通常，一个完整的入侵检测系统包括的基本组件如图 1 所示。

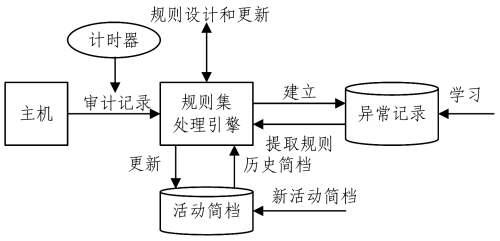

图 1　通用入侵检测系统模型

Fig. 1　General intrusion detection system model

3.2　入侵检测方法

对于网络的各种攻击入侵，如果系统能够将它们迅速、高效地检测出来，就可以使得系统免遭各种不必要的资源以及网络空间的浪费，使其更好地运行，进而通过系统为用户和网络提供更为安全可靠的服务。大量专家学者从不同方面提出了许多机制下的入侵检测方法，如混沌理论[4]、多元相关分析[5]、行为分析、模式匹配、生物免疫系统、神经网络、专家系统、数据挖掘、遗传算法、统计方法[6]和时间序列分析[7]的方法等。这些方法的优劣不同，所应用的情形也不相同。它们不同程度地提高了处理的效率和有效性，能够满足一定的需求。

由于网络中各种攻击存在许多的未知和不确定性，在网络数据流量中往往存在着大量的不确定性和语言值信息，因此在建立入侵检测系统的模型时必须对其客观存在的不确定性进行描述和处理。关于入侵检测的研究也是基于不确定性理论开展的，而直觉模糊理论就是利用直觉模糊知识进行的一种不确定性理论研究。IFTS 模型可以十分有效地描述预测问题中具有模糊、不确定性或者语言值的变量，它们对处理不确定信息系统建模问题具有更大的灵活性和更强的说服力。

本文通过上文总结的网电空间系统中网电攻击现有的技术与手段，尝试把直觉模糊集理论与时间序列预测模型引入入侵检测技术；利用 IFTS 预测模型对各种攻击进行检测；通过将网络流量的特征属性进行直觉模糊化，建立一种新的检测机制，并将其具体应用到网电空间系统中，这也是一种新的尝试。

4　IFTS 预测模型的构建

4.1　直觉模糊集理论

模糊集(Fuzzy Sets，FS)理论最早是由美国加州大学伯克利分校的 Zadeh 教授于 1965 年提出的，主要包括模糊集合理论、模糊逻辑、模糊推理和模糊控制等方面的内容。由于具有较强的客观性以及良好的结合性，模糊集理论一经提出就得到了广泛的研究与应用，主要有直觉模糊集、L-模糊集、区间值模糊集、Vague 集理论等。Zadeh 模糊集丰富的理论研究，促进了其在科学发展中的应用。直觉模糊集理论的研究最为丰富，也拥有更高的关注度。

直觉模糊集最初由保加利亚学者 Atanassov 于 1986 年提出[8]。其完整地定义了直觉模糊集以及直觉模糊理论中基础运算法则和定理的相关内容，尤其是“直觉模糊逻辑”这一基本概念的提出，为直觉模糊集理论奠定了基础。时间序列分析是一种有效的网络流量分析工具，传统的时间序列预测方法主要是以 ARIMA 模型[9]为代表的基于统计分析的方法。

4.2　直觉模糊时间序列模型

时间序列分析研究序列数据的关联性，通过历史数据挖掘序列的变化规律，从而完成对未来数据的预测工作。时间序列分析的基本过程主要为：通过挖掘历史数据的内在变化规律，建立起序列数据所遵从的函数关系，进而对序列在未来的发展做出预测。

定义 1(直觉模糊时间序列)　设给定论域 $X(t)(t=1,2,\cdots)$为 R 的一个子集，$f_i(t)=\langle \mu_i(X(t)),\gamma_i(X(t))\rangle(i=1,2,\cdots)$为定义在 $X(t)$上的直觉模糊集，若

$$F(t)=\{f_1(t),f_2(t),\cdots\} \tag{1}$$

称 $F(t)$为定义在 $X(t)$上的直觉模糊时间序列。

定义 2(高阶直觉模糊时间序列)　令 $F(t)$为定义在 $X(t)$上的直觉模糊时间序列。若 $F(t)$是由 $F(t-1),F(t-2),\cdots,F(t-k)$共同推导得到的，则它们之间的直觉模糊逻辑关系可表示为：

$$F(t-k),\cdots,F(t-2),F(t-1)\rightarrow F(t) \tag{2}$$

称 $F(t)$为 k 阶直觉模糊时间序列。

定义 3(直觉模糊时间序列关系)　对于一个直觉模糊时间序列 $F_l(t)$，如果其仅由前一时刻 $F_l(t-1)$决定，则称其为

一阶时间序列，表示为 $F_I(t)=F_I(t-1)\circ R_I(t,t-1)$，其中$\circ$表示直觉模糊合成操作算子，$R_I(t,t-1)$表示直觉模糊关系矩阵，并且 $R_{ij}=\langle R(\mu_{ij}),R(\gamma_{ij})\rangle=F_I(t)^{\mathrm{T}}\circ F_I(t-1)=[R_{ij}]_{r\times r}$。如果 $F_I(t)$的隶属度函数与非隶属度函数分别为$\langle\mu_{1i},\gamma_{1i}\rangle$和$\langle\mu_{2i},\gamma_{2i}\rangle$，则隶属度和非隶属度关系矩阵的计算式如式(3)所示：

$$R(\mu_{ij})=\bigvee_{k=1}^{r}(\mu_{1ik}\wedge\mu_{2ik})$$
$$R(\gamma_{ij})=\bigwedge_{k=1}^{r}(\gamma_{1ik}\vee\gamma_{2ik}) \tag{3}$$

如果 $F_I(t)$由前 m 个值 $F_I(t-1),F_I(t-2),\cdots,F_I(t-m)$决定，则称 $F_I(t)$为 m 阶直觉模糊时间序列，关系表达式如式(4)所示，其中$\times$是笛卡尔乘积。

$$F_I(t)=F_I(t-1)\times F_I(t-2)\times\cdots\times F_I(t-m)\circ R_I(t,t-m) \tag{4}$$

5 基于 IFTS 的检测算法

5.1 检测模型算法的构造

模型构建的基本过程为：通过计算网络数据流量特征属性的直觉模糊预测误差，来区分正常流量和入侵攻击，建立入侵检测框架，从而达到检测预警的目的。在基于直觉模糊时间序列预测模型的入侵检测方法中，对网络流量的特征属性直觉模糊化是此预测模型方法的关键。

5.2 基于 IFTS 预测模型的入侵检测算法

在时间序列模型中，将网络数据流量看作 k 维的序列数据集，每一维表示数据流量的一种特征属性。为了表示网络数据流量中的语言值特征属性(协议、服务状态)，通过直觉模糊化对不同类型的数据进行处理。下面建立基于 IFTS 预测模型的检测算法，具体步骤如下：

Step1 用 $x_1^k,x_2^k,\cdots,x_n^k$ 来表示网络数据流，k 表示网络数据的特征属性的维数。

Step2 将连续变量的特征属性按照如下直觉模糊化公式进行直觉模糊化，并将离散变量或者语言值变量数据直接划分为直觉模糊集。

$$\langle\mu_j,\gamma_j\rangle=\langle\frac{j-1}{n}+\left|\frac{x_i-d_j}{n(d_{j+1}-d_j)}\right|,1-\frac{j-1}{n}-\left|\frac{x_i-d_j}{\lambda n(d_{j+1}-d_j)}\right|\rangle \tag{5}$$

Step3 训练阶段，将检测算法部署在正常网络流量数据上，针对每一维的流量数据特征属性分别建立一个 IFTS，并且由 m 个历史数据预测得到当前状态。

Step4 根据式(6)计算每一维 IFTS 的预测值 $\hat{x}_n$ 和实际值 x_n 之间的直觉模糊预测误差(Intuitionistic Fuzzy Forecasting Error，IFFE) ε_i，将 IFFE 作为正常流量检测的限定值。

$$\varepsilon_k=\hat{x}_n^k-x_n^k=(\mu(\hat{x}_n^k)-\mu(x_n^k)+(\gamma(\hat{x}_n^k)-\gamma(x_n^k))/2) \tag{6}$$

Step5 攻击检测阶段，将未知的网络流量数据直觉模糊化为 IFTS，根据 m 阶历史数据和直觉模糊关系来计算当前的状态，并计算每一维特征属性的直觉模糊预测误差。

Step6 计算加权预测误差 $\varepsilon_w=(\alpha_1\varepsilon_1+\alpha_2\varepsilon_2+\cdots+\alpha_k\varepsilon_k)$，其中$\alpha_1+\alpha_2+\cdots+\alpha_k=1$，权重分配协同调节各个特征属性对异常检测的影响。

Step7 与正常网络流量训练限定值进行对比，当预测误差值持续超出期望范围时，产生一次攻击警报。

入侵检测算法的基本流程如图 2 所示。

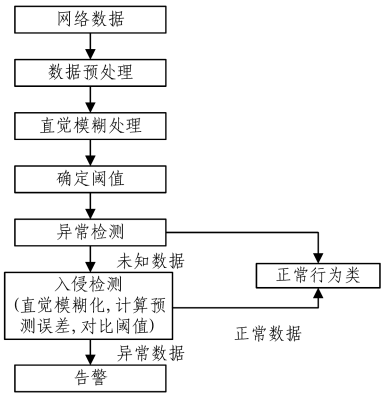

图 2 基于 IFTS 预测模型的入侵检测算法的流程

Fig. 2 Flow of intrusion detection algorithm based on IFTS forecasting model

6 实例研究

6.1 实验环境描述

本文通过实验室的相关设备进行仿真实验，以模拟一个抽象的、简化的网电空间对抗模型。具体过程为：通过将 3 台交换机作为网络的中心节点来分别组网模拟不同的工作域，同时将它们相互连接组成一个可仿真的简化对抗系统模型。具体的方法包括：

1)将指挥协调交换机与上级指挥中心的计算机相互连接；

2)在 3 台不同域交换机下连接对应的 ATM 交换机；

3)将 6 台计算机分别根据各自所属的模拟作战工作域，通过对应的 ATM 交换机相互连接。

在 7 台计算机上模拟用途和类别不相同的对抗工作站需预先安装相关模拟训练软件；并根据实际对抗流程，在 7 台计算机之间，以连续、周期性的方式进行数据传输，从而实现模拟网电空间对抗过程的目的。在本文建立的模型中，选择 3 个不同域的中心节点交换机开展入侵检测工作。

入侵检测的基础是数据，为了能够实时地检测网络数据，本文基于 Winpcap 函数库在 Visual Studio 2013 开发平台上编写了一个用于采集和查看网络数据的抓包工具，以实时采集网络数据。

将检测率(Detection Rate，DR)和误报率(False Positive Rate，FPR)作为入侵检测的性能指标。

检测率＝正确检测出的入侵样本数/入侵样本总数

误报率＝将正常行为检测为入侵行为的样本数/正常行为样本总数

6.2 实验数据与实验结果分析

通过对比系统审计记录、系统日志和实时网络通信数据，结合 Metaspolit 网络攻击平台的攻击数据库，得出目前网电对抗中共 4 大类 38 种常见的异常网络数据。

在实验中，部署在实验计算机上的数据采集模块(即上述

的抓包工具）收集实验网络环境中的各种正常或异常的网络数据，并根据入侵检测模型对数据的维度特征进行处理，生成训练样本集。在对入侵检测系统模型进行充分训练之后，依旧利用抓包工具捕获当前的网络数据包，并对其进行相关检测。采集到的网络数据经数据预处理后得到一组包含 21 个特征共 25223 条训练样本的训练数据集，数据集的构成如表 1 所列。

表 1　训练数据集的攻击行为及分布

Table 1　Attack behaviors and distribution of training data set

攻击类别	攻击类型	训练数据集
Normal	normal	8900
Dos	back	2119
	neptune	6731
	smurf	4282
	maibomb	1327
R2L	guess_passwd	60
	sendmail	14
U2R	buffer overflow	36
	xtem	13
Probe	ipsweep	769
	nmap	175
	portsweep	651
	mscan	147
总计		25223

入侵检测实验的检测平台选用 CPU 3.60 GHz，8 GB 内存，Windows XP 操作系统和 Matlab 2014b 语言编程环境，连接在指挥协调交换机上进行实验。实验结果如表 2 所列。

表 2　入侵检测系统的检测率

Table 2　Detection rate of intrusion detection system

攻击类别	检测率/%	攻击类型	检测率/%
Normal	98.4	normal	98.4
Dos	97.31	back	97.09
		neptune	98.11
		smurf	97.73
		maibomb	96.29
R2L	14.49	guess_passwd	14.87
		sendmail	13.30
U2R	36.83	buffer overflow	42.23
		xtem	27.31
Probe	95.16	ipsweep	95.78
		nmap	93.96
		portsweep	95.49
		mscan	92.77

由上述实验结果可知，本文所提入侵检测方法可以检测到所有类型的攻击；同时，某种攻击的训练样本数量会影响到对这种攻击的检测率，如训练样本数量较少的“buffer overflow”攻击。可以看出，本文方法对各种攻击均具有较高的检测率，但对 R2L 和 U2R 类别攻击的检测率还较低。通过分析可知，R2L 和 U2R 攻击不像 DoS 攻击那样在数据记录中具有频繁序列模式，一般都是嵌入在数据包的数据负载中，单一的数据包和正常连接几乎没有区别，因此本文所提出的检测模型对 R2L 和 U2R 攻击的检测率难免会降低，这也将成为今后研究的重点内容。需要补充的是，由于此类攻击类型在网电对抗过程中出现的概率相对较低，且可以经过人工筛检的方法轻松地鉴别出来，因此，综上所述，本文所提出的入侵检测方法可以有效地应用到网电对抗系统中。

结束语　在信息化条件下的军事斗争和信息技术密集的防空作战领域中，可以预见，网电空间的攻防对抗将异常激烈。本文针对防御体系中的入侵检测提出了一种新的方法和构想，即基于 IFTS 预测模型的入侵检测方法。该方法可以有效地处理语言值或模糊变量；通过不同特征属性对正常流量数据进行报警门限训练；根据 IFFE 指标对多种类型的入侵进行检测；通过加权计算调整不同特征属性的敏感度，以进一步提高模型的检测率。通过搭建网电空间对抗模型，验证了该方法的有效性。该方法对于网电空间对抗防御体系的完善具有一定的指导意义和应用价值。

参 考 文 献

[1] 李为民，黄仁全，王春阳，等. 防空体系反制网电攻击概论[M]. 北京：解放军出版社，2013.

[2] PEDRO M P，PEDRO C，HUMBERTO B，et al. Image segmentation using Atanassov's intuitionistic fuzzy sets [J]. Expert Systems with Applications，2013，4(1)：15-26.

[3] CHANDOLA V，BANERJEE A，KUMAR V. Anomaly Detection：A Survey[J]. ACM Computing Surveys，2009，41(3)：1-58.

[4] CHEN Y H，MA X L，WU X Y. DDoS Detection Algorithm Based on Preprocessing Network Traffic Predicted Method and Chaos Theory[J]. IEEE Communications letters，2013，17(5)：1052-1054.

[5] TAN Z Y，JAMDAGNI A，HE X J，et al. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis [J]. IEEE Transactions on Parallel and Distributed Systems，2013，25(2)：447-456.

[6] LI H Z，GUO S，LI C J，et al. A hybrid annual power load forecasting model based on generalized regression neural network with fruit fly optimization algorithm [J]. Knowledge Based Systems，2013，37(2)：378-387.

[7] THANASIS V，ALEXANDROS P，CHRISTOS I，et al. Real-time Network Data Analysis Using Time Series Models[J]. Simulation Modelling Practice and Theory，2012，29(29)：173-180.

[8] MENG F Y，CHEN X H. Entropy and similarity measure of Atanassov's intuitionistic fuzzy sets and their application to pattern recognition based on fuzzy measures [J]. Pattern Analysis & Applications，2016，19(1)：11-20.

[9] LIPPMANN R P，INGOLS K W，SCOTT C，et al. Evaluating and Strengthening Enterprise Network Security Using Attack Graphs：ESC-TR-2005-064[R]. MIT Lincoln Laboratory，2005.

[10] HUANG X W，ZHANG C. Techniques for intrusion detection based on adaptive intuitionistic fuzzy reasoning[J]. Journal of Computer Applications，2010，30(5)：1198-1201. (in Chinese)
黄孝文，张弛. 基于自适应直觉模糊推理的入侵检测方法[J]. 计算机应用，2010，30(5)：1198-1201.

[11] AHMAD I，ABDULLAH A，ALGHAMDI A，et al. Optimized Intrusion Detection Mechanism using Soft Computing Techniques[J]. Telecommunication Systems，2013，52(4)：2187-2195.

[12] LENG G，MCG I，PRASAD G. Design for self organizing fuzzy neural networks based on genetic algorithms [J]. IEEE Transactions on Fuzzy Systems，2006，14(6)：755-766.

[13] TARTAKOVSKY A G,POLUNCHENKO A S,SOKOLOV G. Efficient Computer Network Anomaly Detection by Changepoint Detection Methods [J]. IEEE Journal of Selected Topics in Signal Processing,2013,7(1):4-11.

[14] YANG Y H,HUANG H Z,SHEN Q N,et al. Reserch on intrusion detection based on Incremental GHSOM[J]. Chinese Journal of Computers,2014,37(5):1217-1224. (in Chinese)
杨雅辉,黄海珍,沈晴霓,等. 基于增量式 GHSOM 神经网络模型的入侵检测研究[J]. 计算机学报,2014,37(5):1217-1224.

[15] FU M B. A Intrusion Detection System Based on Cluster Analysis[J]. Software Engineering,2016,19(4):10-12. (in Chinese)
付明柏. 一种基于聚类分析的入侵检测模型[J]. 软件工程,2016,19(4):10-12.

[16] LI J,DENG G,LI H,et al. The relationship between similarity measure and entropy of intuitionistic fuzzy sets[J]. Information Sciences,2012,188(1):314-321.

[17] ASKARI S,MONTAZERIN N. A high-order multi-variable Fuzzy Time Series forecasting algorithm based on fuzzy clustering[J]. Expert Systems with Applications,2015,42(9):2121-2135.

(上接第 129 页)

[5] GOYAL V,JIAN A,PANDEY O,et al. Bounded ciphertext policy attribute based encryption[C]// International Colloquium on Automata, Languages, and Programming. Berlin, Heidelberg: Springer Press,2008:579-591.

[6] WATER B. Ciphertext-policy attribute-based encryption:An expressive,efficient,and provably secure realization[C]// International Workshop on Public Key Cryptography. Taormina: Springer,2011:53-70.

[7] HINEK M J. Attribute-Based Encryption with Key Cloning Protection[J]. Cryptology Eprint Archive Report,2006,2008(4):803-819.

[8] RUJ S,NAYAK A,STOJMENOVIC I. DACC:Distributed Access. Control in Clouds[C]// 2011 IEEE 10th International Conference on Trust,Security and Privacy in Computing and Communications. Changsha:IEEE Press,2011:91-98.

[9] CHEN J,LIM H W,LING S,et al. Shorter IBE and signatures via asymmetric pairings [C]// International Conference on Pairing-Based Cryptography. Cologne: Springer Press, 2012: 122-140.

[10] LEWKO A B,WATERS B. New proof methods for attribute-based encryption:Achieving full security through selective techniques [C]// Advances in Cryptology-CRYPTO. Santa Barbara: Springer Press,2012:180-198.

[11] CHASE M. Multi-authority attribute-based encryption[C]// The Fourth Theory of Cryptography Conference (TCC 2007). Berlin,Heidelberg:Springer Press,2007:515-534.

[12] CAOZ F. New directions of modern cryptography [M]. Boca Raton:CRC Press,2012.

[13] LEWKO A B,Waters B. Decentralizing attribute-based encryption [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn: Springer, 2011:568-588.

[14] TANG Q,JI D Y. Multi-authority verifiable attribute based encryption[J]. Journal of Wuhan University(Science Edition), 2008,54(5):607-610. (in Chinese)
唐强,姬东耀. 多授权中心可验证的基于属性的加密方案[J]. 武汉大学学报(理学版),2008,54(5):607-610.

[15] LEWKO A,WATERS B. Decentralizing attribute-based encryption[C]// Advances in Cryptology-EUROCRYPT. 2011: 568-588.

[16] YANG K,JIA X H. Attributed-based Access Control for Multi-authority System in Cloud Storage[C]// 2012 IEEE 32nd International Conference on Distributed Computing Systems. Macau: IEEE Press,2012:536-545.

[17] YANG K,JIA X H. Expressive,Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage[C]// IEEE Transactions on Parallel and Distributed Systems. IEEE Computer Society:IEEE Press,2013:1735-1744.

[18] ROUSELAKIS Y,WATERS B. Efficient statically-secure largeuniverse multi-authority attribute-based encryption [C]// International Conference on Financial Cryptography and Data Security. Berlin,Heidelberg:Springer Press,2015:315-332.

[19] YANG X D,YANG M M,YANG P,et al. A Multi-authority Attribute-Based Encryption Access Control for Social Network [C]// 2017 3rd IEEE International Conference on Control Science and Systems Engineering (ICCSSE). Beijing: IEEE Press, 2017:671-674.

[20] FENG D G,CHEN C. Research on Attribute-based Cryptography[J]. Journal of Cryptologic Research,2014,1(1):1-12. (in Chinese)
冯登国,陈成. 属性密码学研究[J]. 密码学报,2014,1(1):1-12.

[21] CAO Z F. New Development of Cryptography[J]. Journal of Sichuan University,2015,1(47):1-12. (in Chinese)
曹珍富. 密码学的新发展[J]. 四川大学学报,2015,1(47):1-12.

[22] CHEND W,WANL Q,WANG C,et al. A Multi-authority Attribute-based Encryption Scheme with Pre-decryption[C]// 2015 Seventh International Symposium on Parallel Architectures,Algorithms and Programming (PAAP). Nanjing: IEEE Press, 2015:223-228.

[23] HU P,GAO H Y. Key-Policy Attribute-Based Encryption Scheme for General Circuits[J]. Journal of Software,2016,27(6): 1498-1510. (in Chinese)
胡鹏,高海英. 一种实现一般电路的密钥策略的属性加密方案[J]. 软件学报,2016,27(6):1498-1510.

[24] BEIMEL A. Secure schemes for secret sharing and key distribution[J/OL]. Phd Thesis Israel Institute of Technology Technion, 1996. http://www. dphu. org/uploads/attachements/books/books_1542_0. pdf.

[25] LIU Z,CAO Z F,WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[C]// IEEE Transaction on Information Forensics and Security. IEEE Signal Processing Society:IEEE Press, 2013:76-88.