基于免疫聚类的入侵检测研究

钟 将 吴开贵 吴中福 李 季 欧 灵
(重庆大学计算机学院 重庆400044)

摘 要 现代网络中用户的行为以及网络结构不断发生变化,因而需要大量已标记的样本数据,用以动态更新入侵检测模式。但是通过手工方式标记学习数据集非常耗时,因此基于标记数据集的检测模型就越来越难以满足实际应用的需要。本文提出了一种使用无标记数据集的基于免疫聚类的异常检测算法,该方法可直接用于检测入侵行为,也可作为建立入侵检测模型的中间步骤,用来提高入侵检测系统的适应性和部署效率。

关键词 异常检测,免疫聚类,异常因子

Intrusion Detection Based on Immune Clustering

ZHONG Jiang WU Kai-Gui WU Zhong-Fu LI Ji OU Ling
(College of Computer,Chongqing University,Chongqing 400030)[1]

Abstract Traditional intrusion detection methods lack extensibility in face of changing network configurations as well as adaptability in face of unknown attack types. Meanwhile, current machine-learning algorithms need labeled data for training first, so they are computational expensive and sometimes misled by artificial data. In this paper, a new detection algorithm, the Intrusion Detection Based on Immune Clustering algorithm, is proposed. It can automatically establish clusters and detect intruders by compute the outlier factor of each data item. Computer simulations show that this algorithm is effective for intrusion detection.

Keywords Abnormal detection,Immune clustering,Outlier factor

1 引言

随着网络连接的迅速扩展,特别是Internet广范应用,越来越多的系统正遭到入侵攻击的威胁。因此如何有效地保证计算机系统的安全就是一个亟待解决的问题。Heady将入侵定义为"任何企图破坏资源完整性、保密性和可用性的行为"[1]。

对于异常行为模式和正常行为模式之间叠加程度的认知不同,目前的检测方法主要分为误用检测和异常检测两类。前者认为两种行为空间相互迭加,不能通过行为特征数据加以区分。而后者认为两种行为模式的特征数据存在显著差异。这两种检测方法各有优缺点,在不同的安全策略下有不同的应用。误用检测不能有效地对检测未知入侵模式,而当前的入侵类型日益复杂,新的入侵行为层出不穷,使得异常检测在入侵检测研究中受到了更大的关注。

入侵检测技术实质上归结为对安全审计数据的处理,这种处理可以针对网络数据,也可以针对主机的审计记录或应用程序的日志文件。目前常采用统计技术、分类技术(决策树,神经网络)、数据挖掘技术来实现异常检测。

由于一般的网络环境内,正常行为是主流,而入侵则表现为个别现象,因此获得的正常实例的规模远大于入侵行为数目。因此可以合理地假设入侵行为相对于正常行为(主流的行为模式)是一些孤立的异常数据。本文基于免疫聚类算法来发现和标记这些孤立的异常行为。

2 研究现状

文[2]采用基于统计方法的异常检测,该方法假设数据的每一个属性维是符合正态分布,那么每一个对象距离聚类中心的距离符合chi-square(χ^2)分布,因此如何检测异常数据的核心问题就是如何估计每一个聚类簇的中心和形状,然后通过χ^2分布特性检测异常数据。文中还给出了一种稳健的参数估计方法,但由于网络特征数据集的每个属性维并不一定满足正态分布,因此在实际应用过程中发现漏检率和误报率偏高的问题。

文[3]给出了一种在大数据量情况下的异常检测技术,该方法的核心思想是通过抽样技术来聚类并发现异常数据,其关键技术是采用基于偏置的抽样方法,使得在密度高的和稀疏的区域采用较高的抽样概率,避免了有价值信息的损失(如聚类中心或者异常数据),该方法实质上是一种基于密度的异常检测方法,即那些分布密度稀疏的区域就是异常数据。但是在网络特征数据集中往往存在分布密度很高的异常数据区域以及密度较低的正常数据区域。

文[4]提出了在检测异常数据时需要根据对象邻近区域的分布模式的情况来确定,文中将数据分布特征分成均匀分布和随机分布和聚类簇三类分布,在异常检测时首先确定其所在区域的分布模式。文中提出了一种识别这三种分布模式的评估方法。该方法综合了密度方法和统计方法来实现异常数据的标识,因此对于不同分布特性的数据集具有较好的适应性。但由于网络特征数据的分布难以采用上述的三种分布

钟 将 讲师,博士生,主要研究方向为网络安全、免疫计算。吴开贵 副教授,博士后,主要研究方向为密码学,网络安全。吴中福 教授,博士生导师,主要研究方向为计算机网络与通、宽带综合业务数字网。李 季 博士生,主要研究方向为免疫计算,网格计算。欧 灵 博士生,主要研究方向为移动代理,网络安全。

模式来刻画每一个簇的分布模式，因此其检测效果也不是很理想。

文[5]提出了采用基于分布密度的聚类和异常(噪音)数据的检测方法，该文中提出了一种密度估计的方法以及密度可达的概念。那么数据集分为核心密度对象和非核心密布对象，然后通过密度可达关系实现聚类，那些不能连接到核心密度对象上的数据就被认为是噪音数据(异常数据)。由于该方法的主要的目的是识别数据集的结构，另外网络特征数据集中存在大量异常的核心密度对象，因此该方法具有较高的漏报率。

文[6]提出了一种基于距离的异常检测方法，该方法不仅适合于正态分布的数据集，而且对于任意分布的数据都可以有效地检测其中包含的异常数据。经过理论分析可知，对于正态分布的数据集，该方法和基于统计的方法具有一致性，两种方法采用的参数是可以相互转换的。由于此方法不需要数据集严格地服从某种分布，因此大量的研究工作都基于这种方法。该方法用于异常检测存在的问题，只能有效地发现全局异常的数据，对于局部异常数据则难以检测。

文[7]的异常检测过程采用聚类-检测两个阶段进行异常数据检测，该算法的思想是将数据聚类后得到的簇集合分成 Large 和 Small 两类。所谓 Large 簇就是指那些数据项最多的几个簇，这些簇包含了超过整个数据集中某个百分比(例如75%)的数据项，剩余的其它的簇就是 Small 簇。对于不同的簇采用不同的局部异常因子(LCF)计算公式。数据项对应的 LCF 越大就越有可能是异常数据，因此该方法可以根据用户指定的参数调节要检测的异常数据的数量。但是方法需要选择适当的方法对数据集的属性进行离散化处理。

3 基于免疫聚类的异常检测算法

3.1 误报容忍因子

衡量一个 IDS 最重要的指标是检测率、误检率和漏检率。假设 I 表示入侵行为；$\overline{I}$ 表示正常行为；A 表示 IDS 发出了报警；$\overline{A}$ 表示 IDS 未发出报警；实际的入侵概率为 $P(I)$，正常行为的概率为 $1-P(I)$。

检测率(Detection Rate)定义为 $P(A/I)$，即发生入侵行为时发出报警的概率；

误报率(False Positive Rate)定义为 $P(A/\overline{I})$，即没有发生入侵行为时发出报警的概率；

漏报率(False Negative Rate)定义为 $P(\overline{A}/I)$，即发生入侵行为时没有发出报警的概率。

在实际的入侵检测系统总是尽可能高地提高检测率，并尽可能降低系统的误报率，但通常情况下这两种指标是相互矛盾的，即提高检测率就会导致误报率的上升。高的误报率导致管理人员的工作强度提高以至于无法有效地响应，而检测率太低会带来的更大的风险，如果存在入侵行为而 IDS 不告警，那么 IDS 就有可能沦为摆设。

为了便于用户根据需要调节系统的性能，本节使用误报容忍因子 α，其定义为 $\alpha=P(A)/P(I)$，即报警数目与实际的入侵的数量的比值。在误报容忍因子 α 条件下的误报率定义为：

$$P_w(\alpha)=\frac{(P(A)-(\alpha-1)*P(I))}{(P(\overline{I})-(\alpha-1)*P(I))}$$

3.2 异常因子

假设用一个 p 维的特征向量集 $X=\{x_1,x_2,\cdots,x_n\}$ 来描述连接行为的网络特征数据集，其中 n 为网络连接数量，$x_i=(x_{i1},x_{i2},\cdots,x_{ip})^t$，$i=1,2,\cdots,n$ 描述其中一次连接的属性特征。为了标识网络连接特征数据集中的异常数据，本节定义了一种新的异常因子计算方法。

由于一般的网络环境中，正常行为是主流，而入侵表现为个别现象，因此获得正常实例的规模要远大于入侵行为，即在正常行为簇中应包含较多的实例，而且这些簇之间不可能偏离很远。本文就是利用这些先验知识来定义和识别网络特征数据集中的异常数据。

定义1 主簇(main cluster) 假设 $C=\{C_1,C_2,\cdots,C_k\}$ 为聚类算法获得的簇的集合，如果簇 C_m 满足 $|C_m|=\max\limits_{1\leqslant j\leqslant k}(|C_j|)$，其中 $|C_j|$ 表示簇的大小，那么 C_m 就是数据集的主簇。

记 c_m 为聚类簇 C_m 的聚类中心，r_m 为主簇的半径。则 $c_m=\sum\limits_{x_j\in C_i}x_j/|C_m|$，$r_m=\max\limits_{x_j\in C_i}(\|x_j,c_m\|)$。其中 $\|x_j,c_m\|$ 为两个向量之间的欧氏距离。

定义2 全局异常簇(global abnormal cluster)，如果某个簇中包含的对象数量小于用户指定的某个值 M 或者聚类中心到主簇中心的距离大于 $N\times r_m$，其中 N 为用户指定的一个常数。

根据定义，全局异常簇要么严重偏离代表主流行为的主簇，要么是位于极其稀疏的区域。因此包含在全局异常簇的数据项就被认为是全局异常数据。

定义3 正常簇 (normal cluster)，如果一个聚类簇不是全局异常簇且其协方差矩阵(covariance matrix)非奇异，那么该簇就是一个正常簇。

根据协方差矩阵不奇异的条件，一个正常簇中至少包含 $p+1$ 个据项。

定义4 异常因子(outlier factor)，对于一个数据项 x_i，其异常因子用函数 $OF(x_i)$ 表示：

$$OF(x_i)=\begin{cases}+\infty \text{ if } x_i\in C_j, C_j \text{ is global abnormal cluster}\\ \min\limits_{C_j\in L}((x_i-c_j)^T\sum\nolimits_j^{-1}(x_i-c_j)), \text{otherwise}\end{cases} \quad (1)$$

位于全局异常簇中的对象，其异常因子无穷大；对于其它簇中的对象，其异常因子为距离所有正常簇的最小马氏距离。其中 c_i 为簇 C_i 的聚类中心，$\sum_j^{-1}$ 为 C_i 的协方差矩阵的逆阵，L 为正常簇的集合，x^T 表示向量的转置。

由于采用了马氏距离(Mahalanobis distance)来计算异常因子，因此兼顾了每个簇的形状，从而比直接使用欧氏距离更能反映数据对象与各个簇间的偏离度。

3.3 算法过程

网络特征数据集中包含了未知数量的聚类簇，且数据集中包含了大量的孤立点，因此使用传统的 K-Means 算法不能有效地解决网络特征数据集的聚类问题。本文利用文[8]中设计的免疫聚类算法对网络特征数据进行聚类分析，然后采用本文定义的异常因子来筛选数据集中的异常数据。

人工免疫聚类算法中一个重要的参数是免疫抑制阈值 t_s，本文中采用经验公式3来计算该值，其中 p 表示数据集属性维的数量，$\|x_j-x_i\|$ 表示两个数据项间的欧氏距离。对于实际的聚类应用应根据评估函数来调整此参数[7]，本文则直接采用公式3的结果。

$$d_i=\sum_{j=1}^{n}(\|x_j-x_i\|e^{-|x_j-x_i|})/(\sum_{j=1}^{n}e^{-|x_j-x_i|}) \quad (2)$$

$$t_s=\sqrt{p}(\sum_{i=1}^{n}d_i)/n \quad (3)$$

由于数据集中不同属性值的范围不同，导致某些特征的权重过大，因此在进行分析之前需要对数据进行规范化处理。

本文采用以下的方法进行数据规范化处理。

$$m_j=\frac{1}{n}\sum_{i=1}^{n}x_{ij} \tag{4}$$

$$\delta_j=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_{ij}-m_j)} \tag{5}$$

$$x'_{ij}=(x_{ij}-m_j)/\delta_j \tag{6}$$

规范化后，使用正交变换保证属性维之间相互独立性。假设经过规范化处理后的数据集为 X'，Σ 为新数据集的协方差矩阵，通常 Σ 不是一个奇异矩阵，因此必然存在一个单位正交矩阵 V 和对角阵 D 满足：$\Sigma=VDV^T$。对规范化后的数据集采用正交线性变换 $X''=X'V$，那么在数据项间距离不变的情况下，消除了属性维之间的关联关系。以下是免疫聚类异常检测算法过程的描述。

算法1　基于免疫聚类异常检测算法

步骤1：对数据集进行规范化处理以及正交线变换得到数据集 X''；

步骤2：使用经验公式(2)计算免疫抑制参数 t_r；

步骤3：采用免疫聚类算法对 X'' 进行聚类分析，并获得簇的集合 C；

步骤4：标识聚类簇集合中的主簇，全局异常簇以及正常簇集合 L；

步骤5：根据定义4计算每一个数据项的异常因子；

步骤6：根据异常因子从高到低筛选和标记异常数据。

4　仿真实验

数据来源：实验数据集为 KDD Cup 1999网络连接数据集[10]。此数据集是1998年在麻省理工学院 Lincoln 实验室由 DARPA 举办的为入侵检测模型评估而建立的测试数据集。该数据集源于美国空军局域网的仿真环境，每个实例包含42个属性，均已标识为正常或特定的攻击行为。数据集中入侵类型按攻击手段类型可划分为以下四类：

DOS-拒绝服务，如 TCP 同步报文洪泛攻击；

U2R-超级用户未授权访问，如缓冲区溢出；

R2L-远端未授权访问，如猜测口令；

PROBE-系统漏洞探测，如端口扫描。

在实验过程中从仿真试验数据集中随机抽取1/10的数据集构造10个试验数据集，其中每一个数据集包含1000个样本数据，其中5个数据集中包含的各种攻击的数量见图1。

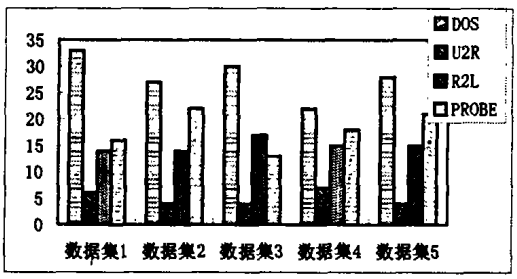

图1　数据集中各种攻击类型的数量

试验结果以及分析：由算法过程可知，影响算法性能的参数有免疫抑制阈值 t_r，判断全局异常簇的参数 M 和 N，误报容忍因子 α。由于篇幅限制，本文仅列举 $M=2$，$N=3$ 条件下的部分计算结果。误报容忍因子 α 以步长为0.1从1增加到3，算法在数据集1和数据集3上试验结果（见图2和图3）。对于不同入侵类型的影响见图4和5。

对实验结果的分析发现：随着容忍因子的增大，总的检测率呈上升的趋势，并且在 $\alpha=3$ 附近能够识别几乎所有的异常数据，且在该容忍因子下的误报率保持在0.5%左右。

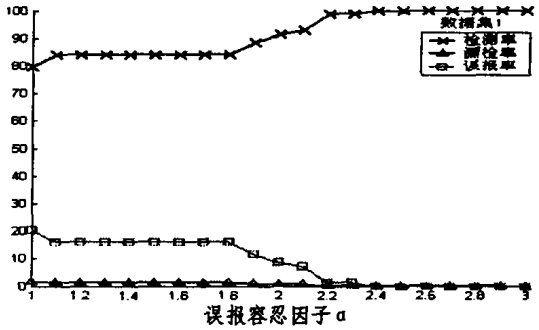

图2　数据集1上的试验结果

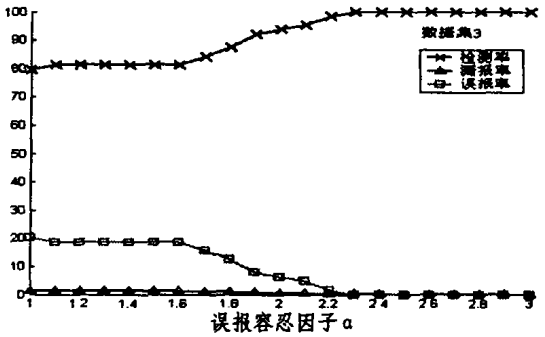

图3　数据集3上的试验结果

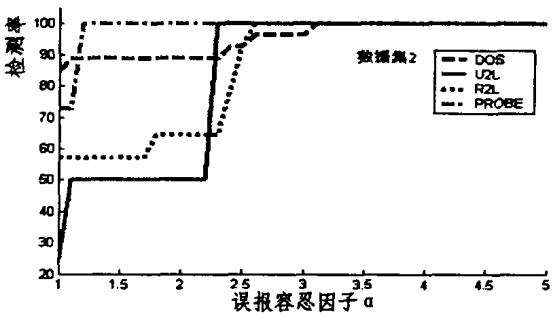

图4　数据集2按入侵类别的检测率

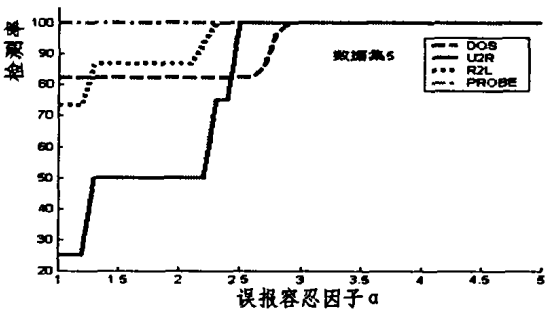

图5　数据集5按入侵类别的检测率

同时发现 α 对于不同入侵类型的影响是不同的。如图4和图5所示的是随着容忍因子的增加，对不同入侵行为的检测率的上升速度的影响是不一致的。对于 PROBE 类型的入侵检测率很快就达到100%，而对于 DOS 类型的攻击在接近 $\alpha=3$ 时才能达到100%。U2L 和 R2L 两种类型的检测率的上升速度介于 PROBE 和 DOS 之间。实际上 PROBE 类型的入侵行为与正常行为之间存在显著差异，因而易于被检测出；而 DOS 则由于和正常行为之间的差异较小，甚至与正常行为集

之间相互覆盖，因此难以被识别。

当入侵行为是小概率事件时，本方法在较小的误报容忍因子下，能够获得理想的检测率。因此在实际的应用中，本方法存在两种应用模式。

1）用于标识网络特征数据集　作为其它有监督学习方法的中间过程，用本方法辅助标记数据集中的异常数据。如果通过专家逐一标记，工作量记为 $O(n)$。由于数据集分为正常和异常两类数据，假设异常数据的比例为 β，通过本方法筛选候选的异常数据集，工作量将下降为 $O(n*\beta*\alpha)$。以 $\alpha=3$，$\beta=0.01$，那么标记效率提高近30倍。

2）用于入侵检测　其应用的基本思路是：利用前面一段时间的网络特征库作为学习数据集，在此基础上建立入侵检测模式。对于当前网络连接，计算其异常因子，如果值不属于异常值的范围内，就认为该连接正常，否则认为是异常连接。此方法的优点是不需要专家标记大量的学习数据集，因此检测模型可以定期地更新，例如每天更新一次，从而适应不断变化的网络环境。主要的缺点是需要管理人员根据分析的结果不断地调整误报容忍因子，以达到理想的检测率和误报率。

小结　本文提出了采用免疫聚类算法提取数据集的结构特征，然后根据定义的异常因子计算每一次连接的异常度。通过在实际网络特征数据集上的实验表明：新方法能够显著地提高标记异常数据的效率，且对于异常行为发生概率较低的环境中可采用本方法直接检测入侵行为。

参考文献

1 Heady R, et al. The architecture of a network level intrusion detection system: [Technical Report CS90-20]. New Mexico: University of New Mexico, Aug. 1990

2 Pell R J. Multiple outlier detection for multivariate calibration using robust statistical techniques. Chemometrics and Intelligent Laboratory Systems, 2000, 52: 87～104

3 Kollios G. Efficient Biased Sampling for Approximate Clustering and Outlier Detection in Large Data Sets. IEEE Transactions on knowledge and data engineering, 2003, 15(5)

4 Hu T, Sung S Y. Detecting pattern-based outliers. Pattern Recognition Letters, 2003, 24: 3059～3068

5 Ester M, et al. A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise. In: Proc. of 2nd Intl. Conf. on Knowledge Discovery and Data Mining (KDD-96)

6 Knorr E M, Raymond. Algorithms for Mining Distance-Based Outliers in Large Datasets. In: Proc. of 24th VLDB conf, New York, USA, 1998

7 He Z, et al. Discovering cluster- based local outliers. Pattern Recognition Letters, 2003, 24: 1641～1650

8 钟将，吴中福，吴开贵，欧灵. 基于人工免疫的动态聚类算法. 电子学报，2004(8)：37～41

9 Kim D J, Park Y W, Park D J. A novel validity index for determination of the optimal number of clusters. IEICE Transactions on Information and Systems, vol. E84-D, 2001(2): 281～285

10 KDD99cupdataset. http://kdd. ics. uci. edu /databases/kddcup99/kddcup1999. html, 1999

（上接第92页）

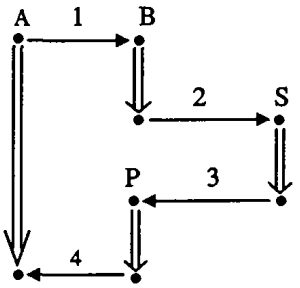

图8　S 发出的消息被 P 拦截

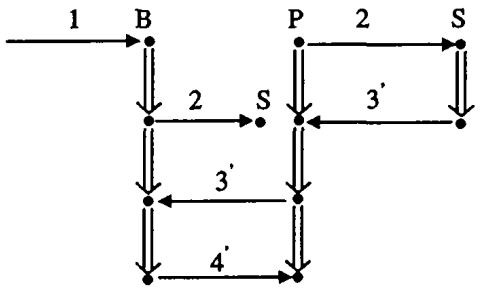

图9　P 的入侵串轨迹

1. $A\rightarrow B: M, A, B, \{N_a, M, A, B\}_{KAS}$
2. $B\rightarrow S: M, A, B, \{N_a, M, A, B\}_{KAS}, \{N_b, M, A, B\}_{KBS}$
3. $S\rightarrow P(B): M, \{N_a, k\}_{KAS}, \{N_b, K\}_{KBS}$
2' $P(B)\rightarrow S: M, A, B, \{N_a, M, A, B\}_{KAS}, \{N_b, M, A, B\}_{KBS}$
3' $S\rightarrow P(B): M, \{N_a, K'\}_{KAS}, \{N_b, K'\}_{KBS}$
3' $P(S)\rightarrow B: M, \{N_a, K'\}_{KAS}, \{N_b, K'\}_{KBS}$
4. $B\rightarrow P(A): M, \{N_a, K'\}_{KAS}$
4' $P(B)\rightarrow A: M, \{N_a, K\}_{KAS}$

攻击结果是 A 得到会话密钥 K，而 B 的会话密钥是 K'。

结论　本文针对串空间理论提出的四条启发式规则在从代数缺陷到实际攻击的转换中非常有效。它们基本上定下了一个攻击转换框架，我们只要在这个框架中填充具体的细节，就可以得到一个实际的攻击描述。但是攻击细节仍然需要我们精心构造，构造的依据是：①遵循代数结论；②根据入侵者的行为模型。

与文[3]不同的是，本文是在人工证明发现缺陷的情况下，启发式的寻找攻击路径。实际转换结果表明本文的启发式规则可以引导我们快速、有效地找到一个攻击过程。这对于研究入侵方法，改造协议是很有帮助的。

参考文献

1 Fábrega F J T, Herzog J C, Guttman J D. Mixed Strand Spaces. In: Proc. of the 12th IEEE Computer Security Foundations Workshop[C], 1999

2 Fábrega F J T, Herzog J C, Guttman J D. Authentication Tests. In: Proc. [C], 2000 IEEE Symposium on Security and Privacy, 2000

3 Song D X, Berezin S, Perrig A. Athena: A novel approach to efficient automatic security protocol analysis. Journal of Computer Security, 2001 (1/2): 47～74

4 Fábrega F J T, Herzog J C, Guttman J D. Honest Ideals on Strand Spaces. In: Proc. of the 11th IEEE Computer Security Foundations Workshop[C], 1998

5 Fábrega F J T, Herzog J C, Guttman J D. Strand Spaces: Why is a Security Protocol Correct. In: Proc. [C], 1998 IEEE Symposium on Security and Privacy, 1998

6 Fábrega F J T, Herzog J C, Guttman J D. Strand Spaces: Proving Security Protocols Correct. Journal of Computer Security[J], 191～230

7 Otway D, Rees O. Efficient and Timely Mutual Authentication. Operating Systems Review[J], 1987, 21(1): 8～10

8 Schroeder N R M. Using Encryption for Authentication in Large Networks of Computers. Communication of the ACM[J], 1978

9 Lowe G. An Attack on the Needham-Schroeder Public-key Authentication Protocol. Information Processing Letters[Z], 1995, 53: 103～107