计算机网络中界壳理论的研究*)

Research on the JieKe Theory in Computer Network

蒋艳凰　蒋贵凰　杨学军

（国防科技大学计算机学院　长沙410073）（北方交大计算机科学与信息技术学院129信箱）

Abstract　JieKe Theory has been presented recently to solve the JieKe phenomenon which exists commonly in the physical word. As the most of other things, computer network has its JieKe phenomenon too. In this paper, we introduce the concept of JieKe first; then we describe the JieKe theory in computer network from two aspects: network concept and its state, and put forward TIS model about network state; using TIS model, we analysis the works of information stream on the development of subnet, discuss the relationship between the security of subnet and JieKe Theory, and evaluate the performance of subnet in a qualitative way. At last, an application about how to evaluate different kinds of firewalls based on TIS model is exploited.

Keywords　JieKe theory, Open radio, TIS model, Firewall

一、引言

当前，网络技术的发展与网络应用的普及对社会进步起着推波助澜的作用，网络已深入到各个领域中。由于每个领域、每个单位都有自己的私有信息，要对外界保密，因此在子网与 Internet 之间就要有诸如防火墙、身份认证等安全措施。这样子网内部就像一个内核，安全控制就是它的外壳，保护着内部不受到侵害。界壳论是曹鸿兴教授最近提出的一门新兴学科，界壳现象在社会和自然界中普遍存在，它在现代计算机网络中也得到了充分的体现。利用界壳理论分析网络的信息流及安全性，从而对网络性能进行评估，这对网络发展起着重要的作用。

二、一般界壳理论

自然界中的众多物体都存在外壳，外壳一方面能够保护自己，一方面又能让物体与外界环境进行交换。这种既能卫护系统的生存和发展，又能司行环境和系统间交换的周界称为界壳。例如：鸡蛋壳、细胞膜、古城墙等，界壳是物体与环境邻接的外围部分。

设系统的周界为 L，其与环境接触的表面积为 ι，界壁 W 所占的面积为 w，界门或通道为 P，所占面积为 p，则显然有：

$$\iota=w+p$$

定义界壳开放度为：

$$\rho=p/\iota=1-w/\iota$$

ρ 越大，系统的开放程度越大，则界壳的卫护作用越小。又记通过界门的实际交换量为 E_s，环境与系统的可交换量为 E_e，则界壳的交换率定义为：

$$\alpha=E_s/E_e$$

它是能量、物质或信息通过界门的能力度量。

三、网络界壳

3.1　网络界壳的引入

现在网络的构建都是众多的园区网与 Internet 相连，园区网内又可分为多个局域网，形成如图1的结构。各个园区网，园区网内的各局域网总有部分信息是私有的，为了保密性的要求，在 Internet 与园区网，园区网与各局域网间都装有防火墙，防火墙保护内部的信息不被外界攻击，同时又让子网内用户能访问外部资源，因此在逻辑上起到了界壳的作用。

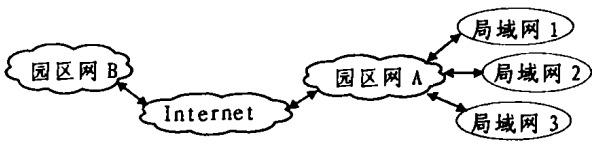

图1　Internet 网络结构

由于防火墙可以做到子网内部对外部的访问与外部对内部的访问不对称，一般内部人员可访问外部数据，而只有部分授权的外部人员才能访问子网内部数据，因此网络界壳的开放度可分为对内开放度 ρ 与对外开放度 γ，其中对内开放度表示内部人员访问外部数据的开放度，对外开放度则相反。

3.2　网络界壳套

如图1所示，园区网 A 与 Internet 之间需设置一层防火墙，形成一个大界壳内。园区网 A 的内部并列套了3个局域网，若在局域网与园区网 A 之间也设置了防火墙，这样就形成了大界壳内并列套有多个小界壳的形式，可以表示为：

$$\{J_i\}\subset\left\{\begin{matrix}J_1\\ \vdots\\ J_i\\ \vdots\\ J_n\end{matrix}\right\}\subset\left\{\begin{matrix}J_1\\ \vdots\\ J_k\\ \vdots\\ J_m\end{matrix}\right\}$$

其中 $i<n<m$。

另一种情况如图2所示，这是 DMZ(DeMilitarized Zone) 形式的防火墙，两个防火墙的中间部分是由两个服务器组成，组成非军事访问区(DMZ)，授权的外部客户可访问此区内的信息，但不能越过非军事访问区获取子网内部信息，这样 DMZ 两端的防火墙必须完成不同级别的安全控制，从而达到子网安全性能的要求。这种系统含有多重界壳套，其形式可表示为：$J_1\subset J_2\subset\cdots\cdots\subset J_n$。这是一种多重单体套。现实中的网络是这两种界壳套的混合使用。

*)本课题得到国家杰出青年科学基金资助(项目编号69825104)。蒋艳凰　博士研究生，主要研究方向为计算机网络安全、图像处理等。蒋贵凰　本科生。杨学军　教授，博士生导师，研究领域为高性能计算机体系结构。

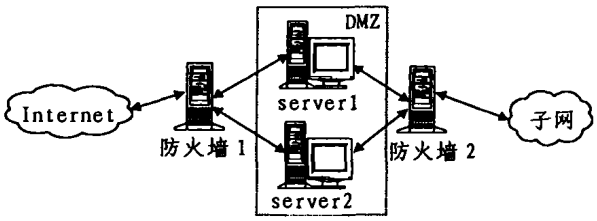

图2 DMZ 防火墙结构

四、网络状态的界壳模型 TIS 及其分析

4.1 TIS 模型的提出

计算机网络状态包括子网自身的发展程度、子网对外界的影响力、子网的安全性三个方面。我们在后面的分析过程中，子网是相对 Internet 而言，前面提到的园区网或局域网都是子网。因此可以将子网的状态用 TIS 模型来描述，此模型可表示为一个三元组(T,I,S)，其中 T：子网内部信息技术总量，即子网自身的发展程度；I：以网络为媒介，子网在外界产生的影响力；S：子网的安全性能。我们可以根据这三个参量的值对子网的性能进行综合评价。

4.2 子网的信息流分析

下面我们利用 TIS 模型来分析一个子网内信息技术的发展。考虑一种普遍且较简单的情况，即认为子网内部人员只能通过该子网访问外部网络，且外部网络对子网的开放度始终为1，也就是说外部网络对子网内部是全透明的，可以随意访问。假设信息技术的发展为指数型，记外部网络对子网信息发展的影响为 F(t)，并令 k 为子网内其它因素产生的信息增长率，则有方程

$$\frac{\partial T}{\partial t}=kT+F(t) \tag{1}$$

记信息梯度为∇T，设 F(t)为扩散型，

$$F(t)=-divJ \tag{2}$$

其中 J 为信息流，我们进一步假定科技流遵循 Fick 律，即

$$J=-\lambda\nabla T \tag{3}$$

将(2)、(3)式代入(1)式，得

$$\frac{\partial T}{\partial t}=kT+\lambda\nabla^2 T$$

由于界壳的存在，从外部网络获取的信息要受界壳的对内开放度 ρ 和交换率 α 的制约，因此可以假设

$$\lambda=b\alpha\rho$$

式中 b 为系数，因此得到在界壳的作用下子网信息技术发展的方程为：

$$\frac{\partial T}{\partial t}=kT+b\alpha\rho\ \nabla^2 T$$

此式用语言可以表示为：子网信息技术的发展等于自身信息技术发展和从外部网络获取信息而引起的信息技术发展这两项之和。k=0表示子网自身的发展处于停滞状态；k 很大，说明仅靠子网内部已有的信息，子网的信息技术也能得到快速发展。αρ=0表明子网不能从外部网络获取任何信息(也可能是物理上隔绝)，这样即使子网与外部网络的信息梯度很大，也不会对子网造成任何影响。

4.3 子网对外部网络的影响

如果某个子网 A 的信息技术发展很快，根据信息的扩散型，就形成向外输出的局面，这时的技术传播可以化为一个扩散问题来求解。由于子网在外界的影响力(即知名度)与子网的信息输出量及由这些输出信息产生的其它信息有关。信息输出量越大，影响力越大；外界在子网输出信息的基础上产生的新的信息技术越多，子网的影响力也越大。我们假设影响力与这两项之和成正比，令这两项之和为 T_e，则有 $I=\beta T_e$。为使问题简化，我们进一步假设空间坐标为一维的，即 x，则有

$$\nabla^2 T_e=\frac{\partial^2 Te}{\partial x^2}$$

则子网 A 向外界产生的影响力方程为：

$$\frac{\partial(\beta T_e)}{\partial t}=c\alpha\gamma\frac{\partial^2 T_e}{\partial x^2}+\eta T_e$$

其中 c 为常定参数，假设 ηT_e 为常定源，且令

$$\zeta=\frac{1}{\beta}=c\alpha\gamma$$

$$k_0=\frac{1}{\beta}\eta T_e$$

则上述方程变为：

$$\frac{\partial T_e}{\partial t}=\zeta\frac{\partial^2 T_e}{\partial x^2}+k_0$$

此方程可进一步写为：

$$\left(\frac{\partial}{\partial t}-\zeta\frac{\partial^2}{\partial x^2}\right)T_e=k_0\delta(x)\delta(t)$$

式中的 δ(·)为狄拉克函数。上式的基本解为：

$$T_e(x,t)=(k_0/\sqrt{4\pi\zeta t})\exp(-x^2/4\zeta t)$$

所以有

$$I(x,t)=(\tau/\sqrt{4\pi\zeta t})\exp(-x^2/4\zeta t)$$

其中 $\tau=\beta k_0=\eta T_e$ 为常定源。在上式中，一方面，ζ 增大，即子网的对外开放度增大，使得 $\tau/\sqrt{4\pi\zeta t}$ 变小，而同时使 $\exp(-x^2/4\zeta t)$ 变大，由于后面是指数型，因此变化大，也就是说若 ζ 增大，将使 I 增大。所以如果子网 A 中的信息让外界访问的多，那么它的影响力也随之增大。

4.4 网络安全

如果子网对外开放度 γ 太大，由于被外界访问的信息过多，在影响力提高的同时，可能会造成保密信息被窃取。网络的安全是由很多不同类型的问题所引起的，我们可以假设共有 n 种类型。由于子网的安全性由子网中最脆弱部分的安全性所决定的，一旦有一点被攻破，可能造成巨大的损失，因此对于只含一层界壳的子网，设这 n 类安全问题中第 i 类所对应的外界攻击强度为 d_i，而界壳相应保护强度为 p_i，则子网的安全性 S 可表示为：

$$S=\theta\left(\min_{1\le i\le n}\left\{\frac{p_i}{d_i}\right\}\right)$$

其中 S 在[0,1]区间取值，S<1表示网络存在安全漏洞，S=1表示网络是安全的。θ 函数为：

$$\theta(x)=\begin{cases}x & \text{当 } x<1\\ 1 & \text{当 } x\ge 1\end{cases}$$

对于含有 m 重界壳的子网，由于每层界壳对子网的保护程度及侧重点不同，对于一类安全问题，只要有一层界壳防住外界的相应的最强攻击，则此类安全攻击就不会对子网造成损害。考虑到 n 类安全问题，则可知子网的安全性为：

$$S=\theta\left(\min_{1\le i\le n}\left\{\max_{1\le j\le m}\left\{\frac{p_{ij}}{d_{ij}}\right\}\right\}\right)$$

其中：P_{ij}为第 j 层界壳对第 i 类安全问题的保护度，d_{ij}为来自第 j 层界壳外部的第 i 类安全攻击度。则可知整个界壳套对第 i 类问题的安全度是所有界壳对该类安全度的最大值，整个子网的安全度等于整个界壳套最脆弱点的安全度。

一般说来，网络的对外开放度 γ 增大，总会导致防火墙某项保护能力下降，因此，根据防火墙当前的各项保护指标适当增大 γ 的值，将会增强子网的外界影响力。

4.5 网络评估与参数分析

根据 TIS 模型，我们可以对网络的性能给出定性的评估。显然，在(T,I,S)中，任何一项的值越大，说明网络的性能越高。

T 越大，即网络的信息含量大，说明该网络发展迅速，信息更新快。但 T 的值受到子网自身信息增长率 k、子网对内开放度 ρ 和信息交换率 α 的制约。提高 k 值关键在于人才的培养；提高 ρ 值主要是要有好的防火墙和网络管理员；另外，就目前的防火墙而言，若提高对内开放度 ρ 和交换率 α，将在一定程度上影响到子网的安全度，因此防火墙技术还有待于进一步提高。

由于外界信息增长率与子网无关，因此 I 值的大小关键在于子网的信息输出量，而这一点受到子网的对外开放度 γ 和信息交换率 α 的制约，γ 和 α 越大，子网的外界影响力越大，但子网的安全度会下降。

由此可见，T，I，S 三项是相互依存、相互制约，在现实中，我们必须找到三者的平衡点，才能构建出最符合要求的网络界壳层。

五、基于 TIS 模型的防火墙方案评价

5.1 方案比较策略

在构建子网时，必须要考虑选取什么形式的防火墙，该防火墙应该具有什么样的功能。因此我们在考虑经费与技术支持的同时，必须对网络的未来状态进行分析预测，选择最适合需求的一种防火墙。

假设对于同一个子网，存在两种不同的防火墙构建方案，选择第一种防火墙其构建困难度（即经费与技术消耗）为 D_1，经过时间 t 后，所对应的网络状态为 (T_1, I_1, S_1)；选择第二种防火墙困难度为 D_2，经过时间 t 后的网络状态为 (T_2, I_2, S_2)，则以第一种方案为基准，将第二种方案与第一种方案进行比较，其值记为 C_{21}，则有：

$$C_{21}=\omega_1\frac{T_2}{T_1}+\omega_2\frac{I_2}{I_1}+\omega_3\frac{S_2}{S_1}+\omega_4\frac{D_1}{D_2}$$

其中 $\sum_{i=1}^{4}\omega_i=1$。同理，第一种方案相对于第二种方案的比较值为：

$$C_{12}=\omega_1\frac{T_1}{T_2}+\omega_2\frac{I_1}{I_2}+\omega_3\frac{S_1}{S_2}+\omega_4\frac{D_2}{D_1}$$

如果 $C_{21}>C_{12}$ 则说明方案二比方案一要好，则选择第二种防火墙。ω_i 为权重，子网对上述的四个方面哪一方面更为重视，相应的权重 ω_i 就越大。由于不同的子网需求不同，因此权重的配置也不相同。

5.2 几种防火墙的比较

下面我们考虑同一子网的防火墙构建方案的选择。由于是针对同一子网，因此可以假设这三种防火墙的界壳交换率相同，即 $\alpha_1=\alpha_2=\alpha_3=\alpha$；子网内由其它因素导致的信息增长率相同，即 $k_1=k_2=k_3=k$；各系数项相同，即 $b_1=b_2=b_3=b$，$c_1=c_2=c_3=c$，$k_{01}=k_{02}=k_{03}=k_0$。也就是说，对于同一子网，使用不同的防火墙只会导致对内开放度 ρ 和对外开放度 γ 不同，以及对于不同的安全问题侧重点不同。考虑到子网要求尽量使网内信息技术增长得快，且尽可能地保证网络的安全，因此可以假设对内开放度均为1，即 $\rho_1=\rho_2=\rho_3=1$，每个防火墙都绝对保证安全，即 $S_1=S_2=S_3=1$。根据以上假设可推出子网内部的信息发展程度相同，即 $T_1=T_2=T_3$。现在我们分析如下三种防火墙的优劣。

第一种方案是 DMZ 形式的防火墙（如图2所示），这种防火墙实际上有两道防护，外部的授权用户经过第一道防火墙的检查可以获取 DMZ 区中信息，任何外部用户都无法越过第二层防火墙窃取子网内部的保密信息。子网可将非保密信息全都送到 DMZ 区的服务器上，供外部用户访问。这样整个 DMZ 形式的防火墙其对外开放度 γ_1 为：

$$\gamma_1=\frac{\text{子网内非保密信息}}{\text{子网内所有信息}}$$

则得该子网的影响力为：

$$I(x,t)=(\tau/\sqrt{\frac{1}{\beta}4\pi c\alpha\gamma_1 t})\exp(-\beta x^2/4c\alpha\gamma_1 t)$$

在这种方案中，两道防火墙都比较容易实现，令其实现难度为 $D_1=D_{11}+D_{12}$，其中 D_{11} 为 DMZ 与 Internet 之间的防火墙构建困难度，D_{12} 为子网与 DMZ 之间的防火墙构建困难度。由于“对外部访问全部禁止”这一功能很容易实现，因此在一般情况下均有 $D_{12}\leqslant D_{11}$。

第二种方案是使用一层防护，为了达到安全的需求，外部用户不能访问内部信息，即 $\gamma_2=0$，因此子网的外界影响力 $I_2=0$。这种防火墙易于构建，它与第一种方案中的第二层防护的构建难度相同，即 $D_2=D_{12}$。

第三种方案也使用一层防护，但是为了增强子网的影响力，允许外部用户访问内部非涉秘信息。这种防火墙的对外开放度与第一种方案相同，因此对外的影响力相同。但是由于在子网内部，保密信息与非保密信息是不加区分的，外部用户在访问子网内部数据时，很可能窃取到秘密信息。为了保证信息不被窃取，防火墙需要设定很多安全检查的功能，而且子网内部信息的组织及安全防护也要大大加强，因此构建困难，耗资很大，网络的安全性不易维护。如果要达到绝对安全，则 $D_3>>D_1$。

由上述分析得到：

$$C_{21}=\omega_1\frac{T_2}{T_1}+\omega_2\frac{I_2}{I_1}+\omega_3\frac{S_2}{S_1}+\omega_4\frac{D_1}{D_2}=\omega_1+\omega_3+(1+\frac{D_{11}}{D_2})\omega_4$$

$$C_{31}=\omega_1\frac{T_3}{T_1}+\omega_2\frac{I_3}{I_1}+\omega_3\frac{S_3}{S_1}+\omega_4\frac{D_1}{D_3}=\omega_1+\omega_2+\omega_3+\frac{D_1}{D_3}\omega_4$$

由于 $I_2=0$，当 $\omega_2\neq 0$ 时，$C_{12}\to\infty$，故 $C_{12}>C_{21}$；又因 $D_3>>D_1$，当 $\omega_4\neq 0$ 时，$C_{13}\to\infty$，则有 $C_{13}>C_{31}$。所以，第一种方案是最佳方案。在经费很紧张，而且子网本身保密性强，不能或不必对外界造成影响力（例如军事单位），也就是说 $\omega_2=0$，则第二种方案是可行的。第三种方案由于耗费太大，不易维护，一般不用。

在实际的 IT 行业中，许多子网并不需要保证绝对安全，只要求子网遭受攻击的概率小于某一值即可，而网络的对外影响力相当重要，这样就可以对第三种方案进行改进，只需保证 $p\leqslant S\leqslant 1(0<p<1)$，这样防火墙的实现难度大大降低。

如果能够确定出子网中这四项的权重，并利用数值求解法得出 T 的数值解，并对所需的防火墙各项性能、指标有明确的要求，从而得出 I、S、D 的值，就可利用这种选择策略求出防火墙的最优方案。

结束语 界壳论是一门新型而又有研究价值的学科，本文将界壳论的思想引入现代计算机网络技术中，并根据界壳理论与当今计算机网络的结构，提出了网络状态模型 TIS，利用 TIS 模型对网络的性能从理论上给予定性的评估，并提出了一种基于 TIS 模型的防火墙选择策略。如果能将界壳论的更深的认识应用于网络乃至整个计算机领域，相信将会有许多新的突破。

参 考 文 献

1 曹鸿兴. 系统周界的一般理论——界壳论. 气象出版社，1997
2 钟云霄. 热力学与统计物理. 科学出版社，1988
3 Internet 防火墙与网络安全. 机械工业出版社，1998
4 Tanenbaum A S. Computer Networks (Third Edition). Prentice Hall International, Inc. 1996
5 Denning D E. Information Warfare and Security. Georgetown University, 1999
6 Grissonnanche A. Security and protection in information systems. Published by Elsevier science publishers B. V, 1989