Journal of System Simulation

Volume 28 | Issue 5 Article 3

7-3-2020

Method for Network Security Reinforcement Based on GSCPN Model

Gao Xiang
1. The Department of Information Operation & Command Training, NDU of PLA, Beijing 100091, China;;2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China;

Liu Yang
1. The Department of Information Operation & Command Training, NDU of PLA, Beijing 100091, China;;

Xiaoyuan He
1. The Department of Information Operation & Command Training, NDU of PLA, Beijing 100091, China;;

Method for Network Security Reinforcement Based on GSCPN Model

Abstract

Abstract: In order to improve the security of networks in whole, a method of making strategies for the network security reinforcement based on Generalized Stochastic Colored Petri Net was proposed. *The concepts of host node utilization index and host node key degree were introduced, which enabled the vulnerable nodes that needed repairing sorted by the value of host node key degree. On this basis, security level of the target network was increased by the reinforcement according to the principle of maximum node key degree first.* The network instance further validates that the proposed method for network security reinforcement is effective, and *the operability is better than traditional methods.*

Keywords

security assessment, GSCPN, modeling, security reinforcement

第 28 卷第 5 期 系统仿真学报© Vol. 28 No. 5
2016 年 5 月 Journal of System Simulation May, 2016

基于 GSCPN 模型的网络安全加固措施制定方法

高翔[1,2]，刘洋[1]，贺筱媛[1]
(1. 国防大学信息作战与指挥训练教研部，北京 100091；2. 数学工程与先进计算国家重点实验室，郑州 450002)

摘要： 为了从整体上提高网络安全性，提出了一种基于广义随机着色 Petri 网模型的网络安全加固措施制定方法。*该方法引入主机节点利用率指数和主机节点关键度等概念，通过计算主机节点的关键度对网络中需要修补的脆弱节点进行排序，在此基础上根据最大节点关键度优先的原则逐步消除网络中存在的脆弱性。*针对网络实例的分析进一步验证了所提出方法的有效性。与传统方法相比，*具有可操作性强的特点,可以指导网络管理人员制定安全加固措施对目标网络进行安全加固。*

关键词： 安全评估；GSCPN 模型；建模；安全加固
中图分类号：TP301 文献标识码：A 文章编号：1004-731X (2016) 05-1009-08

Method for Network Security Reinforcement Based on GSCPN Model

Gao Xiang[1,2], *Liu Yang*[1], *He Xiaoyuan*[1]
(1. The Department of Information Operation & Command Training, NDU of PLA, Beijing 100091, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China)

Abstract: In order to improve the security of networks in whole, a method of making strategies for the network security reinforcement based on Generalized Stochastic Colored Petri Net was proposed. *The concepts of host node utilization index and host node key degree were introduced, which enabled the vulnerable nodes that needed repairing sorted by the value of host node key degree. On this basis, security level of the target network was increased by the reinforcement according to the principle of maximum node key degree first.* The network instance further validates that the proposed method for network security reinforcement is effective, and *the operability is better than traditional methods.*

Keywords: security assessment; GSCPN; modeling; security reinforcement

引言

在互联网迅速发展的同时，各种新型的网络攻击手段也在不断涌现，导致网络信息安全问题变得十分突出。为了保证网络系统的正常运行，就需要对网络进行安全评估，而对网络系统进行建模与分析是网络安全评估中一种行之有效的方法。目前，在网络攻击的建模方面已取得了一些成果。常见的模型有攻击树模型[1]、攻击图模型[2-3]、Petri 网模型[4]等。虽然网络管理人员可以通过这些模型对系统进行脆弱性分析，了解网络系统中存在的脆弱性以及网络安全状况，但仅仅知道这些信息并不能保证网络的安全运行，管理人员还需要更加详细、具有可操作性的网络安全加固措施，并依据这些措施提高网络系统的安全性。

在此方面，Wang 等人[5]提出了一种基于逻辑推理的加固系统安全性的方法，该方法根据网络配置元素求解加固代价最低的安全措施。Jajodia 等人[6]基于攻击图模型对攻击行为进行建模和分析，同时寻找加强网络系统安全的方法。Ma 等人[7]

收稿日期：2014-12-26 修回日期：2016-04-20；
基金项目：国家自然科学基金(61403401, 61374179, 61174156, 61273189, 61174035, 71401168)；军民共用重大研究计划联合基金(U1435218)；全军军事科学研究计划课题(13QJ003-063)；
作者简介：高翔(1984-)，男，辽宁大连，博士，研究方向为网络信息安全与信息系统建模。

提出了一种求解最小费用的加固方法，将加固费用最小化问题转化为一个无约束优化问题。Albanese 等人[8]基于攻击图模型给出了一种计算最优加固措施的近似算法。以上方法大多都是考虑如何为单一主机节点提供安全措施，无法指导网络管理人员提高网络整体的安全性。此外，这些方法主观性较强，制定的网络安全加固措施还不够详细，可操作性也比较差。

为了解决上述问题，本文引入主机节点的利用率指数和主机节点的关键度等概念，给出了相关参数的计算方法。在此基础上，提出了一种基于广义随机着色 Petri 网模型(GSCPN)的网络安全加固措施制定方法，该方法首先求得各个主机节点的关键度，之后在此基础上对需要修补的脆弱节点进行排序，并根据最大节点关键度优先的原则逐步消除目标网络中存在的脆弱性，从而可以从整体上提高网络系统的安全性。

需要说明的是，在文献[9]中，我们给出了广义随机着色 Petri 网模型的定义，并提出了模型的构建算法以及性能等价化简方法，与攻击图、攻击树等评估模型相比，该模型更适于描述并发性和协作性的攻击过程。

1 相关定义

首先给出相关概念和定义。

定义 1 [9]广义随机着色 Petri 网是一个九元组 $GSCPN=(\sum,P,T,F,C,G,E,\lambda,I)$。其中：

$\sum$ 是一组有限非空数据类型的集合，又称为颜色集； P 是有限库所集； T 是有限变迁集，$T=T_t\cup T_i$，$T_t\cap T_i=\phi$，T_t 表示时间变迁集合，T_i 表示瞬时变迁集合；F 是有限弧集，$F\subseteq P\times T\cup T\times P$，且弧仅存在于 P 和 T 之间；C 是颜色函数集，$C:P\to\sum$；G 是条件函数的集合，$G:T\to$ Bool Expression，表示变迁到变迁表达式的映射函数，满足：$\forall t\in T:[\mathrm{Type}(G(t))=\mathrm{Boolean}\wedge\mathrm{Type}(\mathrm{Var}(G(t)))\subseteq\Sigma]$；$E$ 是弧函数的集合，$E:F\to FE$，满足：$\forall f\in F$：$[\mathrm{Type}(E(f))=C(p)_{MS}\wedge\ \mathrm{Type}(\mathrm{Var}(E(f)))\subseteq\Sigma]$，$C(p)_{MS}$ 表示 $C(p)$ 上的多重集的集合；λ 是时间变迁的平均实施速率或瞬时冲突变迁之间优先级集合； I 为初始化函数， $I:P\to\sum$ 为每个库所赋初始颜色。

上述定义中，Type(x) 函数表示 x 的值的类型，Boolean 表示布尔类型，其值为 True 或 False，Var(x) 函数表示 x 中变量的集合。

在本文中，我们令库所集 $p=\{p^i,p^o\}$， p^i 是输入库所， $p^i\in P$，表示攻击者发起时所在的设备的名称和状态； p^o 是输出库所， $p^o\in P$，表示在实行攻击行为后可能所处的位置和状态。T_t 代表时间变迁，表示攻击行为的变迁集合，这里假设攻击行为服从指数分布。

定义 2[9] $\sum$(颜色集)定义为

颜色 Host=string；

颜色 Vul=string；

颜色 AttackCons=SrcHost×DstHost×Vul×Perms；

颜色 SrcHost=Host；

颜色 DstHost=Host；

颜色 Perms={anonymous,guest,root/admin}；

颜色 AttackRes={root access,crash,
confident,compromised...}；

颜色 Conditions=BoolExpression；

颜色 Boolean={true,false}.

其中，攻击条件 AttackCons 由源主机 SrcHost 、目的主机 DstHost 、攻击利用漏洞 Vul 和攻击发起时用户权限 Perms 组成。其中，用户权限 Perms 由匿名 anonymous，授权用户 guest，超级用户 root/admin 组成。攻击结果 AttackRes 由获得主机 root 访问权限(root access)、被攻陷(compromised)、瘫痪(crash) 等组成。 Conditions 是布尔表达式类型，用来表示攻击行为需要的条件。 Boolean 则表示逻辑常量 true 和 false 。

定义 3 主机节点的利用率指数。该指数是对网络攻击中主机节点利用率的度量，记为 $U(\mathrm{IP}\tau)$ $(\tau=1,2...n)$，可以由式(1)得到。主机节点 $\mathrm{IP}\tau$ 的利用率指数越高，说明该节点被攻击的可能性越大。

$$U(\mathrm{IP}\tau)=\sum_{m=1}^{n}a_m^{\tau} \tag{1}$$

式中，a_m 表示在模型稳定状态时攻击发起库所 p_m^i $(m=1,2\cdots n)$ 中平均托肯的数量，$\sum_{m=1}^{n}a_m^{\tau}$ 表示与主机 $\mathrm{IP}\tau$ 对应的 n 个不同的攻击发起库所 p_m^i 中平均托肯数量的累加值。这里的 p_m^i 可以表示攻击者在攻击发起时所处的主机位置，平均托肯数量反映了主机节点在攻击实施过程中的利用率。

定义 4 主机重要度。它用来表示主机节点 $\mathrm{IP}\tau$ 的重要性程度，可以根据主机的类型以及主机所在网络拓扑位置等因素取值，记为 $S(\mathrm{IP}\tau)$。主机 $\mathrm{IP}\tau$ 的重要程度越高，说明该节点的安全性对网络整体安全性构成的影响越大。本文采用了文献[10]量化标准，如表 1 所示。

表 1 网络设备及主机的重要性度量化表

等级	类别	设备重要度
E1	网关或防火墙	5
E2	重要服务器	4
E3	一般服务器	3
E4	重要主机	2
E5	一般主机	1

定义 5 主机节点关键度。对于目标网络中的某个主机节点 $\mathrm{IP}\tau$，它自身的安全性会对网络整体的安全性构成影响，这里将其对网络整体安全性产生的影响称为节点 $\mathrm{IP}\tau$ 的关键度，记为 $HK(\mathrm{IP}\tau)$。

主机的节点关键度由以下两个因素决定：①节点的利用率指数；②主机节点的重要程度。可以由式(2)得到：

$$HK(\mathrm{IP}\tau)=U(\mathrm{IP}\tau)\times S(\mathrm{IP}\tau) \tag{2}$$

定义 6 关键脆弱节点。在目标网络中，按照节点关键度 $HK(\mathrm{IP}\tau)$ 的大小对网络中的主机进行排序，取值最大的一个或者几个节点称为关键脆弱节点。这些脆弱节点对网络安全状况起着最为重要的影响作用，是网络安全加固应该优先考虑的对象。

定义 7 安全加固措施。它主要是指为保护系统资产、减少系统中的脆弱性、抵御网络威胁、降低风险事件的影响，以及打击信息犯罪而实施的各种实践和安全机制，例如修补漏洞和关闭服务等。

2 网络安全加固措施制定算法

在给出上述定义的基础上，本文提出一种基于 GSCPN 模型的网络安全加固措施制定算法，其基本思路如下：

①生成目标网络的 GSCPN 模型；

②将 GSCPN 模型中可以修补或者关闭服务的脆弱节点放入集合 V_R 中；

③计算 V_R 中主机节点的关键度，将 $HK(\mathrm{IP}\tau)$ 取值最大的脆弱节点放入集合 V_C 中；

④重新执行上述步骤，直至 V_R 为空，之后按顺序输出 V_C 中元素。

网络安全加固措施制定算法的实现流程见图 1。

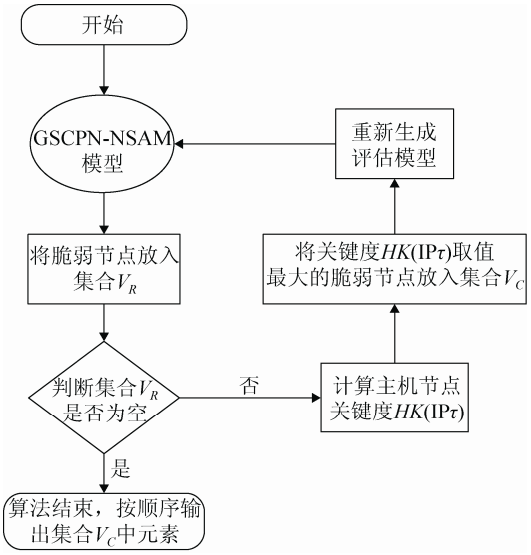

图 1 加固措施制定算法的实现流程

网络安全加固措施制定算法的具体实现如下所示：

网络安全加固措施制定算法

输入：模型相关参数，对应的攻击平均实施速率以及网络主机信息

输出：需要修补或者关闭服务的脆弱节点排序

Step 1：$V_R\leftarrow\varnothing$，$V_C\leftarrow\varnothing$；

Step 2：调用模型的构建算法生成 GSCPN 模型；

Step 3：将可以修补或者关闭服务的脆弱节点放入集合 V_R 中；

Step 4：当 $V_R\neq\varnothing$ 时，调用 CCDHN 算法计算

$HK(\mathrm{IP}\tau)$ 取值最大的脆弱节点；否则，按顺序输出集合 V_C 中元素，算法结束；

Step 5：将集合 V_R 中 $HK(\mathrm{IP}\tau)$ 取值最大的脆弱节点放入集合 V_C 中；

Step 6：调用模型构建算法生成新的 GSCPN 模型，转入 Step 3。

需要指出的是，在利用上述网络安全加固措施制定算法得到的脆弱节点排序序列中，序列中的前一个元素或者 $HK(\mathrm{IP}\tau)$ 取值相同的前几个元素为目标网络中的关键脆弱节点，应该最优先进行安全加固。

CKDHN 算法

输入：GSCPN 模型，攻击路径

输出：$HK(\mathrm{IP}\tau)$ 取值最大的脆弱节点

Step 1：建立攻击路径上出现的脆弱节点集合 $\{\mathrm{IP}\tau\}$ $(\tau=1,2\cdots n)$ 以及原子攻击的攻击发起库所集合 $\{p_m^i\}$ $(m=1,2\cdots n)$；

Step 2：$a_m=0$，$U(\mathrm{IP}\tau)=0$，$S(\mathrm{IP}\tau)=0$，$HK(\mathrm{IP}\tau)=0$；

Step 3：计算 GSCPN 模型稳定状态时攻击发起库所 p_m^i 中的平均托肯数量 a_m，这里的平均托肯数量 a_m 反映了主机设备在攻击过程中的利用率；

Step 4：计算与脆弱节点 $\mathrm{IP}\tau$ 对应的 n 个攻击发起库所中平均托肯数量的累加值，得到该主机节点的利用率指数为 $U(\mathrm{IP}\tau)=\sum_{m=1}^{n} a_m^{\tau}$；

Step 5：根据主机的类型判断主机的重要程度 $S(\mathrm{IP}\tau)$，并由式(2)计算各个主机的节点关键度 $HK(\mathrm{IP}\tau)$；

Step 6：比较每个脆弱节点的关键度，并按照节点关键度的大小对 V_R 中的元素进行排序，输出关键度取值最大的脆弱节点，算法结束。

主机节点关键度计算(calculate the key degree of host node，CKDHN)算法的具体实现如上面所示。算法的第 3 步是计算稳定状态时每个攻击发起库所中的平均托肯数量，具体计算步骤可以参考文献[11]，一般步骤是首先构造与 GSCPN 模型同构的嵌入马尔科夫链，然后基于嵌入马尔科夫链的稳定状态概率进行求解，这里我们采用了仿真工具 PIPE2.5[12]进行相关参数计算，它是由伦敦帝国学院的 Knottenbelt 博士与 David Patterson 领导的研发小组开发的，可以生动和完整地展示 Petri 网，以及计算稳定状态下库所中平均托肯的数量等；第 4 步是将与脆弱节点 $\mathrm{IP}\tau$ 对应的攻击发起库所中的平均托肯数量进行累加，得到该主机节点的利用率指数 $U(\mathrm{IP}\tau)$；第 5 步是根据主机的重要程度 $S(\mathrm{IP}\tau)$，同时结合式(2)计算主机节点的关键度 $HK(\mathrm{IP}\tau)$；第 6 步是对网络中的脆弱节点进行排序，从而可以找到网络危害等级高的脆弱性，这里采用了快速排序方法进行求解，其最坏时间复杂度为 $O(n^2)$，最好时间复杂度为 $O(n\log_2 n)$，同时可以证明该方法的平均时间复杂度也是 $O(n\log_2 n)$。

此外，在实际情况中，如果目标网络规模过大或者较复杂，会导致生成的模型结点数过多，从而影响了算法的性能。为此，我们可以利用文献[11]中的性能等价化简方法对生成的 GSCPN 模型进行化简，即将由同一台主机发起且存在关联关系的两个或者多个原子攻击聚合为一个抽象的攻击，之后再利用上述安全加固措施制定方法对网络的脆弱性进行分析，这样可以大大提高算法的性能。

通过对 GSCPN 模型中主机节点的关键度进行评估，能够帮助我们找出影响网络系统安全的脆弱性。在此基础上，根据求得的脆弱节点排序逐步对网络进行安全加固，这样可以实现提高网络整体安全性的目的。

3 实验与分析

采用文献[13]中的实验网络，其拓扑环境如图 2 所示，主机 IP1 为 Telnet 服务器，主机 IP2 为开放 Ftp 服务的重要主机，主机 IP3 为 Mysql 服务器，主机 IP4 为 Http 服务器。防火墙允许外部访问内部网络主机 IP1，IP2 和 IP3 上运行的服务，并且内部主机之间的访问以及内部主机对外部主机的访问都不受到防火墙的限制。本实验以攻击者控制 3 台主机对主机 IP4 发动拒绝服务攻击为目标。

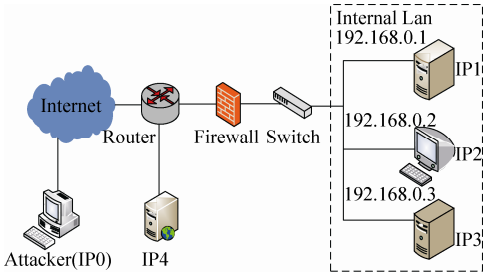

图 2　网络拓扑图

实验网络中主机的漏洞信息如表 2 所示。

生成的 GSCPN 模型如图 3 所示。通过构造该模型的可达树，可以分析得到该模型是完全可达的、有界的、活性的、具有完整性，则该模型是正确、可终止的。

表 2　网络主机相关信息

主机	类别	漏洞信息	服务信息	攻击效果
IP1	一般服务器	Linux7.0 telnet	telnet	Root 权限
IP2	重要主机	ServU5.0	ftp	Root 权限
IP3	一般服务器	Sql 空密码	Mysql	Root 权限
IP4	一般服务器	SYN Flood 漏洞	http	主机瘫痪

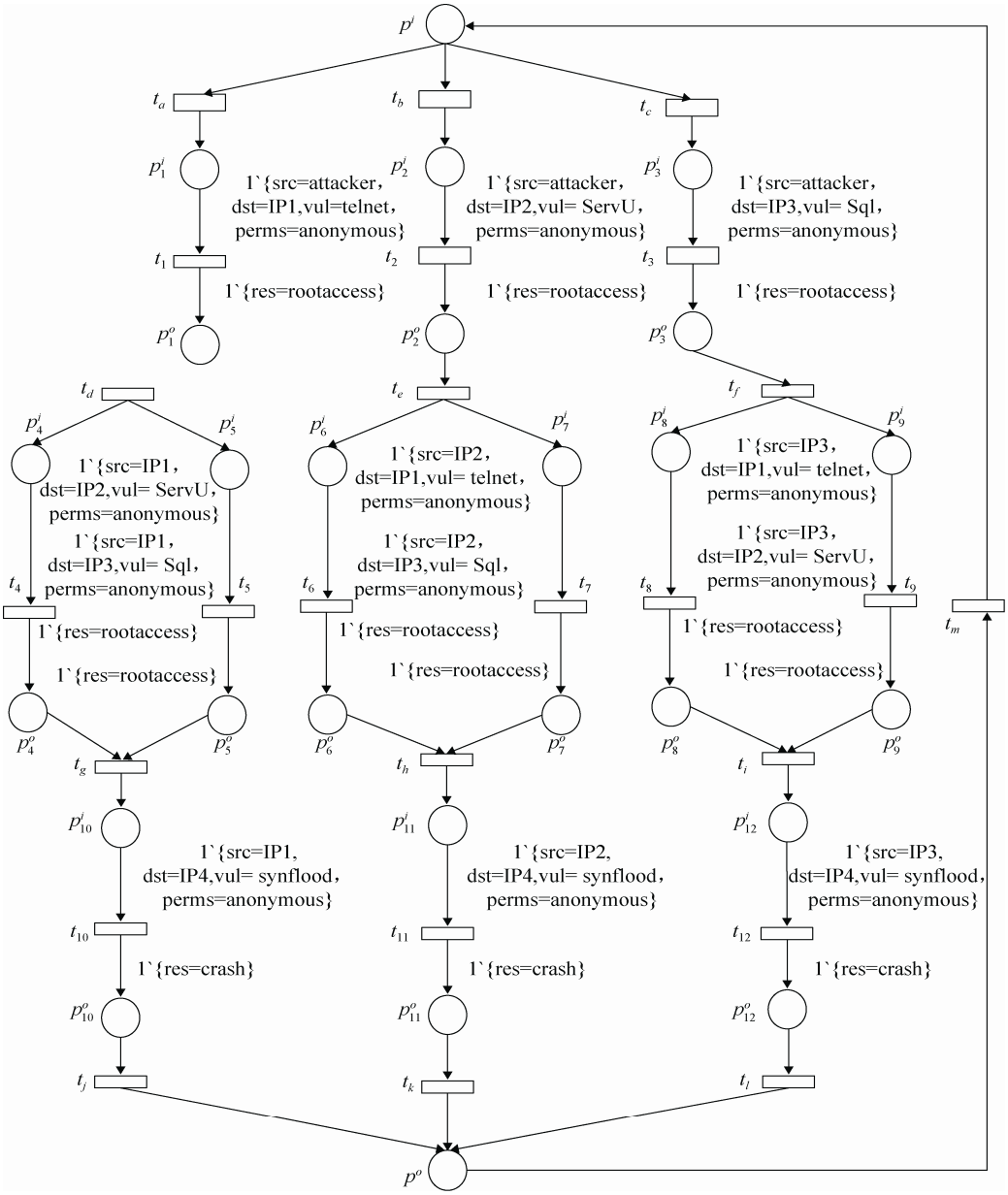

图 3　实验网络 GSCPN 模型

如图 3 所示，p^i 表示发起攻击，p^o 表示到达攻击目标，$p_1^i, p_1^o, p_2^i, p_2^o, p_3^i, p_3^o$ 分别表示攻击者对 IP1，IP2，IP3 进行攻击的前后状态；p_4^i, p_4^o 表示攻击者进入 IP1，攻击 IP2 的前后状态；p_5^i, p_5^o 表示攻击者进入 IP1，攻击 IP3 的前后状态；p_6^i, p_6^o 表示攻击者进入 IP2，攻击 IP1 的前后状态；p_7^i, p_7^o 表示攻击者进入 IP2，攻击 IP3 的前后状态；p_8^i, p_8^o 表示攻击者进入 IP3，攻击 IP1 的前后状态；p_9^i, p_9^o 表示攻击者进入 IP3，攻击 IP2 的前后状态；$p_{10}^i, p_{10}^o, p_{11}^i, p_{11}^o, p_{12}^i, p_{12}^o$ 分别表示攻击者处于 IP1，IP2，IP3，向其它主机发送指令共同实施 DDoS 攻击的前后状态。

瞬时变迁 $t_a, t_b, t_c, t_d, t_e, t_f, t_g, t_h$ 的作用是连接前后两个攻击行为，其中 t_a, t_b, t_c 的转移概率相同。时间变迁 $t_1 - t_{12}$ 对应的攻击平均实施速率分别为 $\lambda_1 - \lambda_{12}$，其中 t_1, t_6, t_8 表示利用 Linux7.0 telnet 进行溢出攻击，并安装 DDoS 攻击木马软件；t_2, t_4, t_9 表示利用 ServU5.0 进行溢出攻击，并安装 DDoS 攻击木马软件；t_3, t_5, t_7 表示利用 Sql 空密码进行攻击，并安装 DDoS 攻击木马软件；t_{10}, t_{11}, t_{12} 表示 DDoS Attack 攻击。

参考美国国家脆弱性数据库(NVD)对相关漏洞攻击复杂度等信息的描述，根据相关的专家经验知识可以设时间变迁 $t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9, t_{10}, t_{11}, t_{12}$ 的平均攻击时间(单位 s)分别为

$$\frac{1}{\lambda_1} = \frac{1}{\lambda_6} = \frac{1}{\lambda_8} = 5，\ \frac{1}{\lambda_2} = \frac{1}{\lambda_4} = \frac{1}{\lambda_9} = 7，$$

$$\frac{1}{\lambda_3} = \frac{1}{\lambda_5} = \frac{1}{\lambda_7} = 3，\ \frac{1}{\lambda_{10}} = \frac{1}{\lambda_{11}} = \frac{1}{\lambda_{12}} = 6。$$

如图 3 生成的 GSCPN 模型中，为了抵御攻击者可能发动的攻击，需要提高安全性的脆弱节点有主机 IP1，IP2，IP3 和 IP4。其中，主机 IP4 上的 SYN Flood 漏洞可以通过禁止主机 IP0 访问来增强防御，所以暂时不考虑对其进行修补或者关闭服务。

基于以上分析，利用本文给出的网络安全加固措施制定算法，我们可以获得目标网络中可能遭受恶意攻击的各个主机节点的节点关键度 $HK(IP\tau)$，如表 3 所示。

表 3 初始的主机节点关键度

主机	节点关键度计算结果
IP1	0.855 51
IP2	0.499 04
IP3	0.962 43

具体计算过程如下：

表 1 中，根据主机的类型可以得到，实验网络中各个主机的重要程度 $S(\mathrm{IP}\tau)$ 分别为 $S(\mathrm{IP1})=3$，$S(\mathrm{IP2})=2$，$S(\mathrm{IP3})=3$。主机节点利用率指数 $U(\mathrm{IP}\tau)$ 可以通过仿真工具 PIPE2.5 计算得到，分别为：

$$U(\mathrm{IP1}) = a_4^1 + a_5^1 + a_{10}^1 = 0.285\,17$$

$$U(\mathrm{IP2}) = a_6^2 + a_7^2 + a_{11}^2 = 0.249\ 52$$

$$U(\mathrm{IP3}) = a_8^3 + a_9^3 + a_{12}^3 = 0.320\,81$$

根据式(2)可得各个主机节点的节点关键度 $HK(\mathrm{IP}\tau)$ 分别为：$HK(\mathrm{IP1}) = U(\mathrm{IP1}) \times S(\mathrm{IP1}) = 0.28517 \times 3 = 0.85551$，$HK(\mathrm{IP2}) = U(\mathrm{IP2}) \times S(\mathrm{IP2}) = 0.24952 \times 2 = 0.49904$，$HK(\mathrm{IP3}) = U(\mathrm{IP3}) \times S(\mathrm{IP3}) = 0.32081 \times 3 = 0.96243$。

通过比较容易看出，主机 IP3 的节点关键度最高，即为关键脆弱节点，所以应该优先对主机 IP3 上的 Sql 空密码漏洞修补或者关闭 Mysql 服务。例如，在修补了 Sql 空密码漏洞后，即使主机 IP3 上运行 Mysql 数据库，也不会对主机 IP3 的安全性产生影响，即攻击者对主机节点 IP3 不可达。因此，下一次生成的模型中将不会包含攻击者利用主机 IP3 实施下一步攻击的攻击行为。

消除主机 IP3 上的脆弱性后，生成的 GSCPN 模型如图 4 所示。重新计算主机节点关键度，可得主机 IP1 的节点关键度最高，为 1.083 33。因此，应该选择修补主机 IP1 上的 Linux7.0 telnet 漏洞或关闭 Telnet 服务。

第 3 次生成的 GSCPN 模型如图 5 所示，在该图中只有一条包括 2 个攻击行为的攻击路径，即攻击者利用了主机 IP2 上的 ServU5.0 漏洞获得系统权限，然后控制主机 IP2 对主机 IP4 发动拒绝服务攻击。消除主机 IP2 上的脆弱性后，再次生成 GSCPN 模型时，集合 V_R 为空，算法结束。

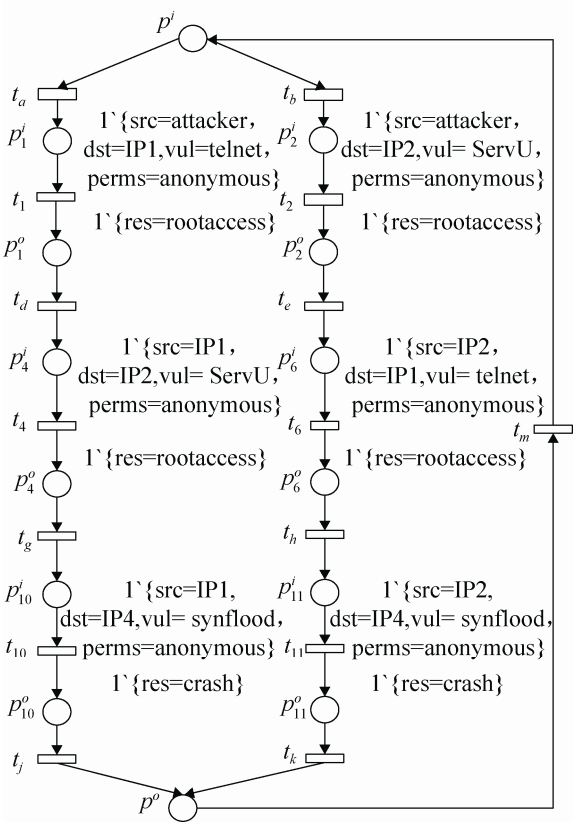

图 4 消除主机 IP3 脆弱性后的 GSCPN 模型

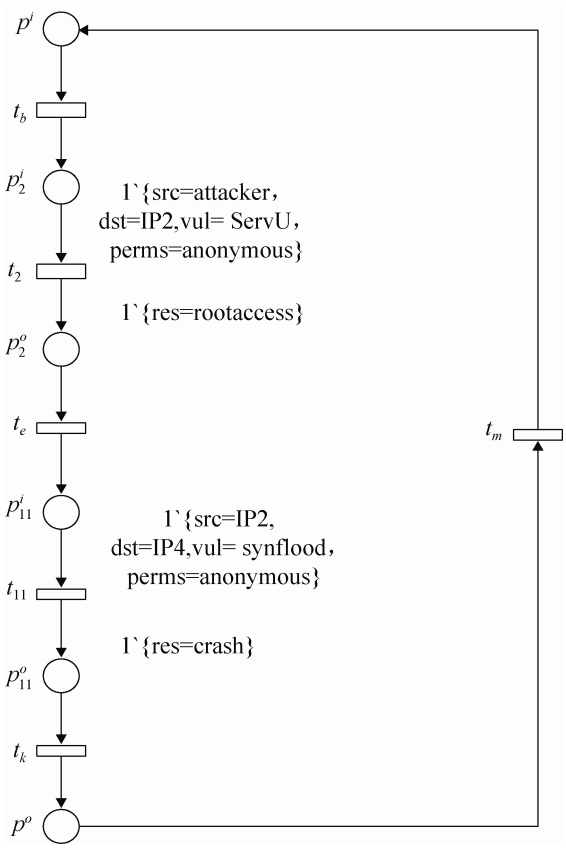

图 5 消除主机 IP1 脆弱性后的 GSCPN 模型

由此可得，为了提高网络的整体安全性，管理人员制定的网络安全加固措施应该是：

(1) 尽力修补主机 IP3 上的 Sql 空密码漏洞或者关闭 Mysql 服务；

(2) 修补主机 IP1 上的 Linux7.0 telnet 漏洞或者关闭 Telnet 服务；

(3) 修补主机 IP2 上的 ServU5.0 漏洞或者关闭 Ftp 服务；

(4) 禁止主机 IP0 访问主机 IP4 上的 Http 服务。

网络管理人员只要根据实际情况选择其中的网络安全加固措施，就可以最大程度地提高网络安全性。

此外，根据本文提出的 CKDHN 算法可得，主机 IP3 为关键脆弱节点，即主机 IP3 自身的安全性对网络整体安全性构成的影响最大，这与实际网络攻击情况相符合。与传统方法[6-8]相比，本文提出的方法具有以下优势：

① 不仅可以为单一主机节点提供具体的安全措施，同时也可以指导网络管理人员逐步提高网络整体的安全性，其制定的策略更详细，具有可操作性强的特点。

② 传统方法大多是基于攻击图和攻击树等模型，它们欠缺对描述并发性和协作性攻击过程描述的能力[9]，而本文的方法是基于 GSCPN 模型，适于对异步、并发的计算机系统建模，可以针对并发性攻击提出有效的网络安全加固措施。

③ 采用定量的分析方法，可通过 Petri 网仿真工具 PIPE2.5 求解相关参数，计算方法相对简单。

4 结论

为了提高网络整体的安全性，本文引入主机节点的利用率指数和主机节点关键度等概念，给出了一种基于 GSCPN 模型的安全加固措施制定方法，并以一个实例验证了所提方法的可行性和有效性。该方法可以通过仿真工具求解相关参数，计算过程简单，可操作性强，能够帮助网络管理人员逐步消除网络中存在的安全缺陷以及隐患。下一步的研究工作：现有的表述方法仍然不够完善，我们要继续

研究如何对网络拓扑结构、主机操作系统类型等参数进行更合理的抽象。

参考文献:

[1] R Dewri, I Ray, N Poolsappasit, et al. Optimal security hardening on attack tree models of networks: a cost-benefit analysis [J]. International Journal of Information Security (S1615-5262), 2012, 11(3): 167-188.

[2] 吴金宇, 金舒原, 杨智. 基于网络流的攻击图分析方法 [J]. 计算机研究与发展, 2011, 48(8): 1497-1505.

[3] S Z Wang, Z H Zhang, Y Kadobayashi. Exploring attack graph for cost-benefit security hardening: A probabilistic approach [J]. Computers & Security (S0167-4048), 2013, 32(2): 158-169.

[4] 吴迪, 冯登国, 连一峰, 等. 一种给定脆弱 性环境下的安全措施效用评估模型 [J]. 软件学报, 2012, 23(7): 1880-1898.

[5] Wang Ling yu, S Noel, S Jajodia. Minimum-cost network hardening using attack graphs [J]. Computer Communications (S0140-3664), 2006, 29(18): 3812-3824.

[6] S Jajodia, S Noel. Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection, and Response [M]. New Jersey, USA: World Scientific, 2009: 285-305.

[7] Ma Jun-chun, Wang Yong-jun, Sun Ji-yin, et al. A Minimum Cost of Network Hardening Model Based on Attack Graphs [J]. Procedia Engineering (S1877-7058), 2011, 15: 3227-3233.

[8] M Albanese, S Jajodia, S Noel. Time-Efficient and Cost-Effective Network Hardening Using Attack Graphs [C]// Proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks, Boston, USA. USA: IEEE, 2012: 1-12.

[9] 高翔, 祝跃飞, 刘胜利. 一种基于广义随机着色 Petri 网的网络攻击组合模型 [J]. 电子与信息学报, 2013, 35(11): 2608-2614.

[10] 司加全, 张冰, 尚大鹏, 等. 基于攻击图的网络安全性增强策略制定方法 [J]. 通信学报, 2009, 30(2): 123-128.

[11] 林闯. 随机Petri网和系统性能评价 [M]. 北京: 清华大学出版社, 2005: 23-35.

[12] N J Dingle, W J Knottenbelt, T Suto. PIPE2: A Tool for the Performance Evaluation of Generalized Stochastic Petri Nets [J]. ACM SIGMETRICS Performance Evaluation Review (S0163-5999), 2009, 36(4): 34-39.

[13] Gao Xiang, Zhu Yuefei, Fei Jinlong, et al. Method Based on GSCPN for Network Vulnerability Analysis [J]. Journal of Software (S1796-217X), 2013, 8(8): 2032-2038.

(上接第 1008 页)

程变得更加简单和明了。所以，基于 DBM-UML 建模方法的 CPS 系统计算实体建模是非常有用并且值得推广的。最后，我们以智能车驱动模块的计算实体建模为例，对本文给出的建模方法进行案例性阐述。

本文给出的建模方法在前人的基础之上进行了改进，使得 CPS 计算实体建模的过程更加合理，对系统的描述更加全面，系统模型更加完善。

参考文献:

[1] 刘子微. CPS 系统的时空 UML 模型建模方法研究 [D]. 上海: 华东师范大学, 2012.

[2] 何积丰. Cyber-physical Systems [J]. 中国计算机学会通讯, 2010, 6(1): 25-29.

[3] 黎作鹏, 张天驰, 张菁. 信息物理融合系统(CPS)研究综述 [J]. 计算机科学, 2011, 38(9): 25-31.

[4] 刘厦, 王宇英, 周兴社, 等. 面向 CPS 系统仿真的建模方法研究与设计 [J]. 计算机科学, 2012, 39(7): 32-35.

[5] Li-na C, Hong-Bin H, Su D. Research on CPS spatio-temporal event model based on the state [C]// Computer Science & Education (ICCSE), 2011 6th International Conference on. USA: IEEE, 2011: 195-198.

[6] Derler P, Lee E A, Vincentelli A S. Modeling cyber–physical systems [J]. Proceedings of the IEEE (S0018-9219), 2012, 100(1): 13-28.

[7] 李晓宇, 王宇英, 周兴社, 等. 一种信息物理融合系统仿真建模方法 [J]. 系统仿真学报, 2014, 26(3): 631-637.

[8] 王明松. UML 图形系统的设计及应用 [D]. 沈阳: 东北大学, 2005.

[9] 郝兆平. 基于 UML 的自来水公司收费管理系统的研究与实现 [D]. 南京：南京理工大学, 2010.