网络安全中协同攻击的威胁评估方法*)

张 峰 秦志光 刘锦德
(电子科技大学计算机学院 成都610054)

摘 要 威胁评估是网络安全分析的重要问题,也是入侵防御和响应的前提。提出了一种基于入侵事件集的威胁评估方法,它综合考虑了攻击次数、攻击源、攻击初始威胁度、被保护目标的重要级别等因素。通过属性聚类分析,得到相关的入侵事件集合,评价事件集的威胁程度。该方法具有一阶线性的计算复杂度,可以对协同攻击事件进行实时威胁评估。

关键词 入侵事件,威胁评估,协同攻击,网络安全

Threat Assessment Method for Coordinated Attacks in Network Security

ZHANG Feng QIN Zhi-Guang LIU Jin-De
(Department of Computer Science of UEST of China,Chengdu610054)

Abstract A major research problem in network security analysis is threat assessment. It's one of premises of protection and response for network security. An event set based threat assessment method is proposed. Clustering the security events results in correlative event sets, which are assessed according to attack frequency, source, initial threat value and the priority level for protected target. The method has first order linear complexity. It can be used in real-timethreat assessment for coordinated attacks.

Keywords Intrustion event, Threat assessment, Coordinated attacks, Network security

1 引言

系统漏洞的存在和攻击工具的广泛传播使得网络攻击更为频繁。其中,协同攻击是威胁较大的一类。协同攻击是精心策划和实施的一组攻击,它通过各个部分的分工协作以达到一个共同的攻击目的。攻击工具更加自动化和智能化,协同攻击日益盛行,但它难于检测和有效防御。在协同攻击的检测方面,出现了一些有代表性的系统。如 UC-Davis DIDS[1]和 GrIDS[2],SRI EMERALD[3],CARDS[4]系统。上述研究集中于协同入侵的攻击建模、入侵检测。对于协同入侵的评估则少有关注。而威胁评估技术是入侵防御和响应的前提和基础,是构成网络安全主动防御体系的重要组成部分。

威胁评估是安全周期中风险管理的一部分,它提供量化入侵事件的威胁程度的方法,为监管系统采取相应的防御措施提供依据。1999年,IAAC(Information Assurance Advisory Council)启动了"信息安全保障的威胁评估与预警方法"项目,研究威胁评估的量化方法和预警方法[5]。协同威胁评估是对一组相关的攻击事件(目标相关,源相关,方法相关,时间相关)进行整体的评估,从而得出攻击事件集对于特定目标的威胁程度,为监管系统提供防御参考。本文研究协同攻击的威胁评估技术,基于简单入侵事件的评估初值,提出一种广义的事件集合的评估方法,可对协同入侵事件进行快速有效的威胁评估。

2 威胁评估算法

首先引入算法中的概念,并对算法中涉及的一些量的计算方法加以说明。然后介绍算法的详细步骤,分析算法的执行效率,并对算法中加权值的赋值方法加以讨论。

2.1 算法基础

定义1 入侵事件,由以下五元组表示:$I=\{D,S,R,C,T\}$。每个入侵事件具有五个属性。其中,D 为目标地址集合,S 为源地址集合,R 为请求服务类型集合,C 为攻击类型集合(文中以 Snort 定义的攻击类型为例),T 为时间标记集合。

定义2 入侵事件集,$E=\{e_i|e_i\in I,i\in N\}$。$E$ 是入侵事件的集合,其中的元素称为项,每一项是一个入侵事件。

定义3 视图 V 是一组聚类条件,V=orExpr | andExpr |groupExpr,其中,orExpr=OR ((D|S|R|C|T)=val). andExpr=AND ((D|S|R|C|T)=val)。条件表达式由项属性、属性值表达式和关系符 OR、AND 的组合构成。视图可以产生具有相同属性值的一组入侵事件集。

在威胁评估中,为了计算特定视图下的入侵事件的频次,采用了一种基于统计信息网格(STING)的多分辨率聚类方法。聚类结果是将相似的记录分成若干组,得到相关目标聚类的入侵事件频次集。入侵事件的属性(目标地址,源地址,请求服务类型,攻击类型,时间)看作 n 维空间 S 的维,分别有一个有界定义域。输入的入侵事件 $e=\{d,s,r,c,t\}$ 为 n 维空间中的点集。聚类方法如下:

确定包含聚类的子空间

利用单调性引理(基于关联规则挖掘的先验性质 apriory property):频繁项集的所有非空子集也是频繁的。设 $k=1$,遍历报警数据库,找出所有的一维密集单元格(攻击)

a 频次大于 minf(事件发生的最小频次),其组成的集合记为 E_1;

b 若 $k<n$ 则由 k 维的密集单元格集合 E_k 生成 $k+1$维的

*)基金项目:863资助项目"战略预警与监管体系结构研究"(2002AA142040)。张 峰 博士生,主研方向:网络安全主动防御技术。秦志光 教授,博导,主研方向:网络安全、办公自动化。刘锦德 教授,博导,主研方向:开放系统与其安全性技术、中间件技术。

候选密集单元格，否则转 d；

c 若 E_{k+1}不为空则，过滤掉非密集的单元格，$k=k+1$，转 b；

d 得到最高维的密集单元格构成的子空间。

回答查询的方式

a 确定与查询相关的聚类子空间的维数 k；

b 从 k 维聚类子空间集合中选择与查询最相关的聚类子空间；

c 只考虑第 k 层中满足查询条件的单元，$k+1$层的处理仅对这些单元进行；

d 重复 c 直到满足查询要求；

e 对最终结果的处理：过滤掉非密集单元格。

以目标 IP 聚类为例，对应的查询方法描述如下：目标 IP 聚类(过去一段时间内各 IP 段内发生的攻击次数)：有确定值的参数只有一个(时间)，故聚类子空间的维数为1。

a 一维聚类子空间包括5个独立的空间(时间)，(攻击源)，(目标)，(请求服务类型)，(攻击类型)，只选择与查询相关的空间，即(时间)空间；

b 时间空间中与查询相关的单元为，时间轴的值在给定时间段内的单元，第二层的处理仅对这些单元进行；

c 在二维聚类空间中选择(时间)一(目标)空间，对 c 得到的单元进行目标 IP 段的划分，得到该时间段内攻击的目标网段分布；

d 过滤掉不满足最小频度值的单元格。

定义4 协同攻击，C 是一组有协同关系的入侵事件集，C 是 E 中的项在某一视图下的集合。设 $C=\{e_1,e_2,\cdots,e_m\}$。

定义5 默认威胁级别，代表单一入侵事件的初始威胁级别。一般说来，这是一个依据单一攻击破坏力、传播范围、攻击工具与手段等因素赋予的一个经验值。文中参考了 Snort 在入侵规则的"priority"字段中定义的默认威胁级别，它将已知的攻击行为划分为32大类，每类攻击具有相近的操作过程或攻击目的。每个大类对应一个1-4级的威胁级别[6]。

定义6 被保护目标(目标主机、请求服务类型)的重要程度 λ，$0<\lambda<1$。

2.2 算法步骤

威胁评估模型用于计算单一攻击或协同攻击的威胁程度。主要包含两个步骤：利用单一攻击事件的默认威胁值，建立初始威胁数据库；对于选定的事件属性视图下的入侵事件集，计算威胁程度。

2.2.1 *建立威胁数据库* 威胁数据库将用于查找特定攻击在发生特定次数时的威胁值，建立方法如下：

a 攻击次数威胁分析：利用聚类的结果，某时间段内攻击越频繁的攻击源威胁程度越大，将攻击频次 f 定义为所分析攻击集合中同种攻击类型的攻击发生的次数，归约到[0.0，1.0]的值域范围内，即可得到攻击源威胁值 x 与 f 的函数关系，记为 $x(f)=f/(1+f)$；

b 攻击源个数威胁分析：考虑到协同攻击时，攻击源的个数同样影响到威胁的程度，攻击源的个数越多，可能发生的协同攻击的威胁程度越大，用同样的方法将攻击源的个数归约成威胁值，记为 $x(m)=m/(1+m)$；

c 确定主要属性(攻击类型)，将其按威胁度分类；

d 估计各属性下攻击源的威胁大小：攻击源在第 n 类攻击类型下的威胁程度，记为 $x(n)$，存入威胁数据库。

2.2.2 *计算入侵事件集的威胁程度* a 识别攻击源，计算其攻击频次 f，得到其威胁程度 $x(f)$；

b 确定不同攻击源的个数 m，得到攻击源个数的威胁值 $x(m)$；

c 由威胁数据库得到攻击源在第 n 类攻击类型下的威胁程度 $x(n)$；

d 根据经验确定攻击频次 f、攻击源个数 m 以及攻击类型 n 的期望威胁度 μ_1、μ_2、μ_3，其值表示了两者对攻击威胁值的影响程度，且 $\mu_1+\mu_2+\mu_3=1$，将其分别作为攻击源和攻击类型威胁权值；计算目标的威胁程度：$X=\lambda[\mu_1x(f)+\mu_2x(m)+\mu_3x(n)]$。

e 对三种输入的不同处理：

若(1) 同一攻击源同种攻击类型的攻击集合：($m=1$)

当 $f=1$时，即单个确定的攻击，

$$X=\lambda[\mu_1x(1)+\mu_2x(1)+\mu_3x(n)]=\lambda[\frac{1}{2}\mu_1+\frac{1}{2}\mu_2+\mu_3x(n)]$$

当 $f>1$时，即同一攻击源多次相同的攻击，攻击频次越大威胁越大，

$$X=\lambda[\mu_1x(f)+\mu_2x(1)+\mu_3x(n)]=\lambda[\frac{f}{1+f}\mu_1+\frac{1}{2}\mu_2+\mu_3x(n)]$$

若(2) 不同攻击源同种攻击类型的攻击集合($m>1$，$f>1$)：该条件下的攻击集合看作协同攻击，其攻击威胁值通过直接计算基本威胁公式获得，即

$X=\lambda[\mu_1x(f)+\mu_2x(m)+\mu_3x(n)]$。

若(3) 不同攻击源不同攻击类型的攻击集合：该条件下的攻击集合由于其关联度无法确定，我们将其分别按同源同类型和异源同类型攻击集合对待，对其分别计算所有可能的威胁度，取最大值作为最终结果。方法如下：

同源同类型攻击划分：区分该集合中所有可能的同源同类型攻击子集。得到 i 个攻击子集，设为 $A_1,A_2,\cdots,A_i$；其次，利用1.的方法分别计算各子集的威胁值 $X_1,X_2,\cdots,X_i$；取最大值 $X^1=\max(X_1,X_2,\cdots,X_i)$。

异源同类型攻击划分：区分该集合中所有可能的异源同类型攻击子集(协同攻击)，将上面得到的 i 个子集 $A_1,A_2,\cdots,A_i$，按照攻击类型分组，如集合 A_q 的攻击为第 t 类攻击，则将划分到第 t 组，得到 j 个组，设为 $B_1,B_2,\cdots,B_j$；其次，利用2.的方法分别计算各组的威胁值 $X'_1,X'_2,\cdots,X'_j$；取最大值 $X^2=\max(X'_1,X'_2,\cdots,X'_j)$。

将所有可能的威胁值取最大值作为最终结果，即 $X=\max(X^1,X^2)$。

2.3 效率分析

威胁数据库的建立依赖于聚类分析的结果，因此计算量由聚类算法而定。若为同一攻击源同种攻击类型或不同攻击源同种攻击类型，计算复杂度为常值；若为不同攻击源不同攻击类型，计算复杂度为 $O(m)$，这里 m 为攻击源个数。这种威胁评估算法有以下特点：(1)将攻击本身的威胁程度和发生的频率计算在内，可以动态地计算一个攻击事件的威胁程度；(2)可以计算协同攻击的威胁程度。可以看到，该算法计算威胁值最高复杂度为一阶线性的，而且较为真实地反映了入侵事件/入侵事件集的实际情况。

2.4 讨论

权值 μ_1,μ_2,μ_3 反映了一组协同攻击中，攻击频次、攻击源个数、单一攻击的威胁程度等对整体攻击的重要程度。至于被保护主机的重要程度由系统管理员根据经验赋值。下面讨论确定 μ_1,μ_2,μ_3 的方法。

取定 a_1,a_2,a_3 三种已知威胁程度的协同攻击，它们对应的威胁评估值分别为 X_1,X_2,X_3

由 $X(f,m,n)=\lambda[\mu_1x(f)+\mu_2x(m)+\mu_3x(n)]$

$$x(f)=\frac{f}{1+f},x(m)=\frac{m}{1+m},x(n)=x(n_{a_i})$$

令 $\alpha_i=\frac{f_i}{1+f_i},\beta_i=\frac{m_i}{1+m_i},\gamma_i=x(n_{a_i})$，得

$$\begin{cases}\alpha_i\mu_1+\beta_i\mu_2+\gamma_i\mu_3=X_i/\lambda,i=1\cdots3,j=1\cdots3 & (1)\\ \mu_1+\mu_2+\mu_3=1,\mu_i\geqslant0 & (2)\end{cases}$$

μ_i 的取值由上述超定方程组确定，解的情况讨论如下。令 $A=\begin{bmatrix}\alpha_1&\beta_1&\gamma_1\\ \alpha_2&\beta_2&\gamma_2\\ \alpha_3&\beta_3&\gamma_3\end{bmatrix}$，式(1)的解可由克莱姆法则判断并求出。设解空间为 $U^*=(\mu_1^*,\mu_2^*,\mu_3^*)$

a. 若 $|A|\neq0$，即(1)式有唯一解，解由克莱姆法则直接给出 U^*，且唯一解 U^* 若在平面(2)上，则超定方程组有唯一解。

b. 若 $|A|=0$，即(1)式有无穷多解。同时，当 Rank(A)=1，则(1)式退化为一个平面，解空间 U^* 由该平面和平面(2)确定，若两平面相交，则解空间为一条直线(多穷多解)，若两平面平行，则解空间为空。

若 $|A|=0$，且 Rank(A)=2，则(1)式退化为一条直线，解空间 U^* 由该直线和平面(2)确定：若直线在平面上，则解空间 U^* 为该直线(无穷多解)；若直线与平面相交，则解空间 U^* 为唯一点；若直线与平面平行，则解空间 U^* 为空。

关于上述超定方程的解，可以借助广义逆矩阵的概念[7]，得到更为简洁的表示形式。

3 应用实例

在承担的863项目"战略预警与监管体系结构研究"中，原型系统应用了上述协同攻击的威胁评估方法。预警系统对已发生入侵事件进行威胁评估，得到攻击与入侵的历史规律，发送给监管系统；预警系统对预测的未来的入侵事件进行威胁评估，提供给监管系统，作为防御参考，提前采取对应的防护措施。

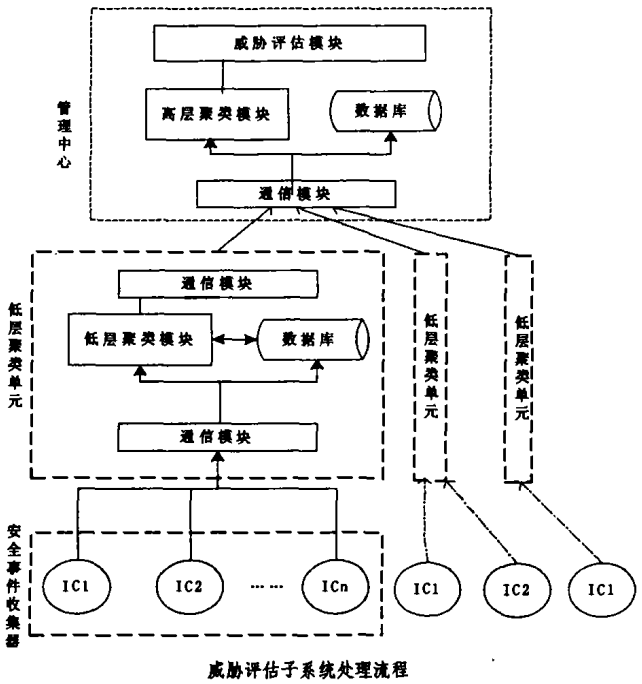

图1 威胁评估子系统处理流程

威胁评估子系统接收来自监控子网的入侵事件收集器的入侵事件信息。由聚类模块实现按主题视图的聚类(区分为相关的入侵事件集合)。为减轻预警中心的负担，将局部入侵事件的聚类计算下移到聚类单元(每组安全相关子网配置一个聚类单元)中实现。而管理中心对局部聚类信息进行二次聚类，得到全局安全信息。对入侵的历史规律也将利用这五种属性的聚类信息。聚类用于低层安全聚类和高层安全聚类分析中。它们采取了相同的算法。威胁评估算法实现在威胁评估模块中。它利用聚类结果提供的攻击频次、指定时间段的攻击源个数、初始威胁库作出威胁评估。在系统测试中，对1000个入侵事件完成5种主题聚类的时间不超过1秒。对协同攻击/入侵事件集的威胁评估是实时的(具有一阶线性的多项式计算复杂度)，可以满足实时威胁评估的需求，也较为客观地反映了相关攻击行为对特定目标的威胁程度。

结论 提出了一种新的威胁评估方法。采用基于 STING 算法的聚类方法计算入侵事件在属性视图下的频数。通过计算初始威胁值、攻击源分布、攻击频次、攻击目标的重要程度等因素，对攻击威胁度加以评估。不仅可用于计算单个入侵事件威胁值，还可用于计算协同攻击入侵事件集合的威胁值，且具有一阶线性计算复杂性。这使得入侵事件的威胁值成为一个可量化的指标，从而能够为其它的安全系统及时有效地提供攻击的威胁信息，使之采取有效的防御措施。这为网络综合防御系统的实施奠定了基础，使得各网络安全组件的联动成为可能。

参 考 文 献

1 Snapp S R, Brentano J, et al. DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype. In: Proc. 14th NCSC: Washington, DC, Oct. 1991. 167～176

2 Staniford-Chen S, et al. GrIDS - A Graph Based Intrusion detection System for Large Networks. In: Proc. 19th National Information Systems Security Conf. Vol. 1, Oct. 1996. 361～370

3 Porras P A, Neumann P G. EMERALD: Event Monitoring Enabling Response to Anomalous Live Disturbances. In: Proc. 20th National Information Systems Security Conf., Baltimore, MD, Oct. 1997

4 Yang J, Ning P, Wang X S, Jajodia S. CARDS: A distributed system for detecting coordinated attacks. In: Proc. of IFIP TC11 Sixteenth Annual Working Conf. on Information Security, Aug. 2000. 171～180

5 Rathmell D A, Dorschner J, Knights M. Project: Threat Assessment and Early Warning Methodologies for Information Assurance. http://www.icsa.ac.uk/Projects/ropa.htmlIAAC, Summary of Research Results: Early Warning & Threat Assessment Methodologies For Information Assurance. http://www.iaac.org.uk/Publications/ROPA/Website%20summary.pdf. May, 2001

6 The Snort Project. Snort Users Manual. http://www.snort.org/docs/snort_manual.pdf. Dec, 2003. 22～24

7 孙继广. 矩阵扰动分析(第二版). 北京：人民邮电出版社，2001. 28～31