基于可信报警事件的在线攻击场景重构算法*)

郭山清　曾英佩　谢　立
(南京大学计算机软件新技术国家重点实验室　南京 210093)
(南京大学计算机科学与技术系　南京 210093)

摘　要　传统的入侵检测系统仅提供大量独立的、原始的攻击报警信息，不利于用户和入侵响应系统对攻击及时做出响应，迫切需要根据低层的报警信息，建立高层的攻击场景，提高安全管理员对当前发生的攻击的认知度。本文利用贝叶斯规则首先对多个安全设备产生的报警信息进行过滤，生成了可信的报警事件集，在此基础上完成攻击场景的重构工作，减少了安全设备产生的误报信息对关联算法的影响，提高了关联算法的健壮性和可扩展性。描述的关联方法可以使报警事件的聚合操作和攻击场景重构同时进行，实现了对报警事件的在线分析功能，弥补了现有算法的不足。试验结果表明，该算法在场景重构和报警事件约减两个方面都表现出了良好的性能。

关键词　入侵检测，攻击场景，关联，贝叶斯规则，事件约减，在线分析

An Online Attack Scenarios Construction Algorithms Based on Delievable Alarms

GUO Shan-Qing　ZENG Ying-Pei　XIE-Li
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract　Traditional intrusion detection systems(IDSs) only provide large amount of independent, low-level attack alerts, though there may be logical connections between them. As a result, it is difficult for users or response systems to understand the alerts and take appropriate actions for these attacks. So it needs to deduce high-level attack scenarios and analysis the attack's objective from low-level attack alerts. This paper uses Bayesian rule to filter the alarm set, produces the believable alarm set and shows the most plausible ones among these possible scenarios based on this set, which decrease the effect of false negative alarm and improve this correlation algorithm's robustness and expansibility. This algorithm can also be used to analysis the online alarm set, which avoid the shortcomings of the existed algorithms. We evaluate this model with DARPA evaluation database, which shows good performance in attack scenario construction and alarm reduction.

Keywords　Intrusion detection, Attack scenario, Correlation, Alarm reduction, Online analysis

1　引言

Dorothy E. Denning1987 年首次提出了入侵检测的概念[1]。经过约 20 年的发展，入侵检测系统取得了长足的进步并获得了广泛的应用，但仍面临着 3 个方面的挑战[2]：1)海量的报警事件；2)严重的误报和漏报；3) 难以根据报警信息诊断系统所存在的漏洞。解决以上问题的一种途径是利用事件关联技术分析海量报警事件，抽取有用的信息，重构整个攻击场景，从而提高报警信息的利用率，降低误报并帮助安全管理员分析出系统所存在的漏洞。

目前已有一些研究机构提出针对报警信息进行关联分析，建立攻击场景的方法[2,3,13,19,20]。文[2, 19]提出利用报警属性之间的相似性，如 IP 地址、端口、时间等属性，进行关联，但只能关联一些简单的事件。文[21,3]提出利用事先已知的攻击场景进行关联分析，它的特点是：对已经分析出来的攻击场景利用某种已定义的语言进行描述，分析的准确率较高，但存在着攻击场景不易描述、构造，不易发现新的攻击场景等缺点。文[20,13]提出利用已知的攻击的前提条件和后果进行攻击信息关联，具有一定的发现新攻击场景的能力，但攻击者在实施一串攻击时，许多攻击之间并没有严格的因果关系，无法通过此方法构造出来，且该方法在建立模式时，空间复杂度比较高，容易引起状态的膨胀。

虽然已经提出众多的关联算法，但现有算法没有充分考虑源报警信息的可信性问题。同时，以上方法都主要分析的是离线的报警信息，导致构造出来的攻击场景具有严重的滞后性。针对存在的不足，本文提出了基于可信报警事件的在线关联算法。

本文第 2 节简单描述与攻击场景有关的基本术语；第 3 节提出在有多个安全设备的环境下攻击场景的重构方法；第 4 节对该算法进行实验验证并做出了基本的分析；第 5 节是相关工作，最后总结全文并概述未来的研究方向。

2　攻击场景的描述

2.1　基本定义

定义 1　报警事件[4]　安全设备检测到系统或网络中发生异常时所产生的警告信息，可表示为一个六元组(Attacktype, Src_Ip, Src_Port, Dst_Ip, Dst_Port, Time_stamp)，其中 *AttackType* 表示攻击类型，*Src_Ip*，*Src_Port* 和 *Dst_Ip*，*Dst_*

*)江苏省自然科学基金(No. BK2002073)和江苏省软件与集成电路专项基金项目《千兆线速网络安全防护系统》。**郭山清**　博士生，主要研究方向：网络安全、机器学习；**曾英佩**　硕士生，主要研究方向：网络安全；**谢　立**　教授，博士生导师，主要研究方向：分布式计算、先进操作系统和信息安全。

Port 分别表示攻击的源目的 IP 地址和源目的端口地址，*Time_stamp* 代表攻击被检测到的时间。

定义 2 攻击场景[13] 定义为一个序列 $S(A_1, A_2, \cdots, A_n, O)$，其中 A_i 是组成攻击场景 S 的攻击实例，A_1 是攻击场景 S 的初始攻击，O 是攻击场景 S 的攻击目的(目标)，组成攻击场景 S 的攻击实例之间必须满足以下条件：

1) $\forall i,j \in \{1,\cdots,n\}$，如果 $i>j$ 则 $A_i.time\_stamp > A_j.time\_stamp$；

2) $\forall i \in \{2,\cdots,n\}$，$\exists j<i$，攻击实例 A_j 将会影响到攻击实例 A_i。

2.2 攻击过程描述

分析报警事件的目的是通过分析安全设备产生的报警信息来获知攻击者的攻击过程(即攻击场景)，进一步识别其攻击意图，而其入侵过程可被看作分阶段的对目标环境直接或间接实施多种攻击手段，逐步达到其攻击目标(完成攻击意图)的有目的的演化过程。在整个攻击过程中，攻击者下一阶段实施的可能攻击动作都由从上一阶段获取到的关于目标环境的知识和攻击者自身所固有的知识及其最终要达到的攻击目标所决定，如图 1 所示。

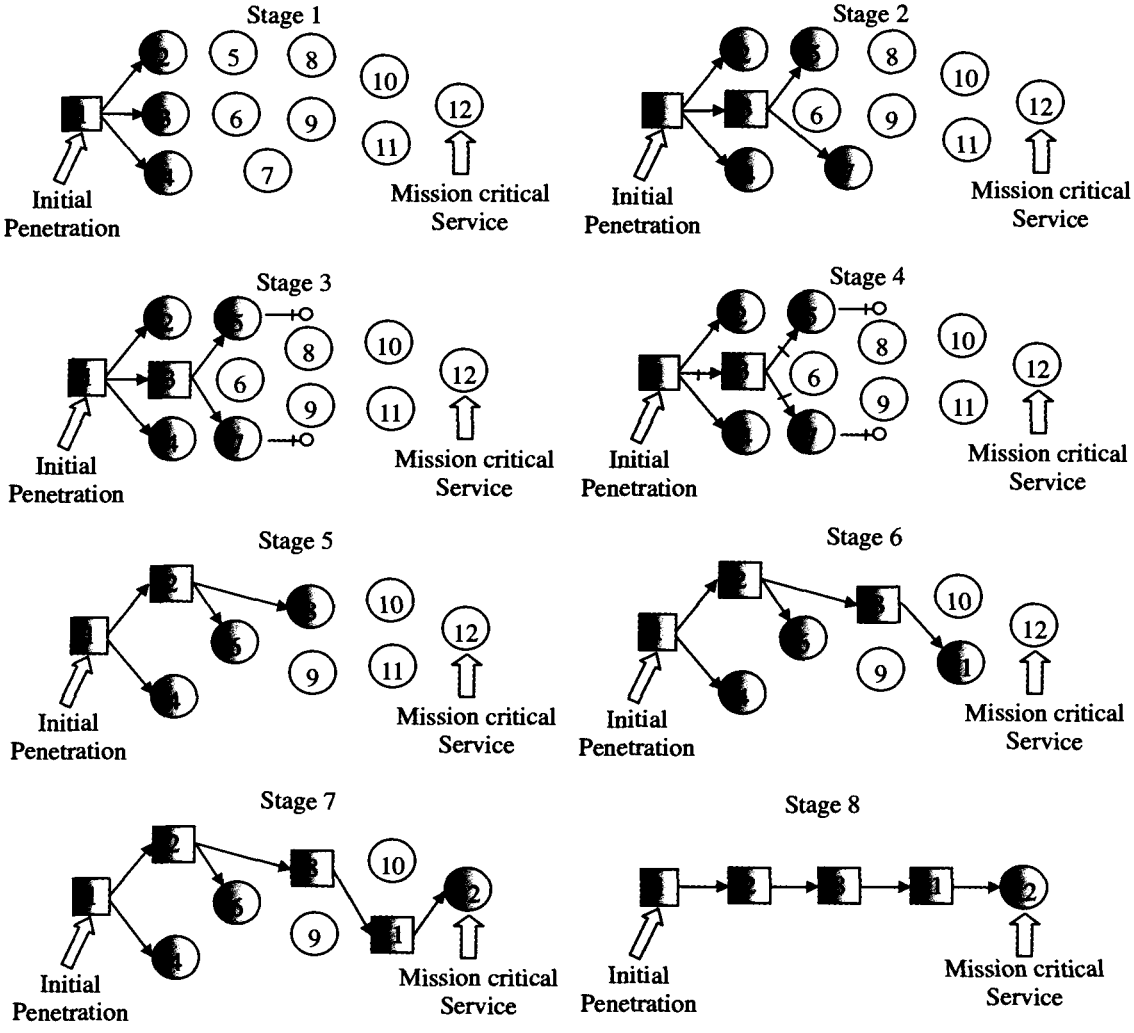

图 1 攻击过程样例图

图 1 展示的是某攻击者为了完成某攻击任务而发动入侵的一个攻击过程实例图。在图 Stage 1～8 中，攻击者发动了攻击 1。在攻击 1 完成后，攻击者可以选择 2,3,4 三种攻击方式做为整个攻击过程的进一步攻击手段。根据个人的经验和偏好，攻击者选择了攻击 3 进行进一步的攻击。而攻击者发现在完成了攻击 3 后，攻击者根据攻击 3 所获取的知识，继续发动攻击 5 和 7 后，发现通过以上手段难于达到攻击目的。因此，作者重新选择攻击 2 进行攻击，然后依次发动攻击 8，11,12，最终成功地达到了入侵的目的。

从上面的分析可以看出，整个攻击过程可以用 $M=(S, \tau, s_0)$ 表示，其中 S 表示攻击过程中的候选状态集，$\tau \subseteq S \times S$ 表示通过攻击手段 τ 完成攻击过程中状态到状态的转换关系，S_0 表示攻击场景的起点。而攻击过程中的某一时刻其状态可以表示为 $S=S_d \cup S_c \cup S_g$，其中 S_d 表示已经达到的攻击状态，S_c 表示候选状态集，$S_g = S - S_d - S_c$ 表示潜在的攻击状态集合。如图 1 中的 Stage1 所示：$S_d=\{1\}$，$S_c=\{2,3,4\}$，$S_g=\{5,6,7,8,9,10,11,12\}$。

3 基于可信报警事件的关联算法

随着安全设备的广泛使用，在一个复杂的网络中，可能存在多种安全设备，而每种设备都会产生种类繁多的报警信息。产生的这些报警信息实际上是依靠安全设备本身的特点从多个角度对当前环境的安全状况做出的判断，所以利用从多个安全设备中产生的报警信息对减轻众多安全设备所产生的报警事件的场景重构的影响有很大的作用。本文主要针对当网络环境中存在多个安全设备的时候，如何更好地利用这些信

息完成攻击场景的重构做了一定的探索。

3.1 关联算法描述

根据以上分析，从报警信息中重现攻击过程实际上可以转换为获取攻击模型 $M=(S,z,S_o)$ 的问题。本文提出了关联算法，在叙述该算法以前，首先给出几个符号表示的意义：

算法：基于可信报警事件的在线攻击场景重构算法

典型符号：

Knowledge：表示攻击者当前的知识；

CandiAttackSet：表示攻击者根据当前攻击者所掌握的知识可能采取的的动作候选集合，即待发生的候选攻击集合；

GrSer=$\{M_1,\cdots,M_N\}$，其中 M_i 是从报警事件中获取的单个攻击模型。

1)接收新的 *Alert*=(Attacktype, Src_Ip, Src_Port, Dst_Ip, Dst_Port, Time_stamp)，利用 3.3 节中描述的算法计算选择可用来进行关联操作的 Alert 集。如果该集合为空，跳转到 1。

2)从 GrSet 中获得在当前时间窗口 W 中发生的攻击状态集合 $S^D=S'_{d,1}\cup\cdots\cup S'_{d,N}$，其中 $S'_{d,i}\subseteq S_{d,i}$，$S_{d,i}$ 为 GrSet 中攻击模型 M_i 中的已经发生的攻击动作。如果 *Alert* 的信息和 S^D 中的某个状态可以匹配，则直接完成报警事件融合操作，然后跳转到 1，否则执行 3。

3) 删除候选攻击集合中在时间窗口 W 以外的备选攻击，然后对候选攻击状态集合 S^C 的每种候选攻击按照其优先级依次计算其与当前发生的报警事件 *Alert* 的匹配程度，其中每种候选攻击的被选择的优先级与其时间戳成正比：即距离当前时间越近，被首先选择到的机会越高。当存在一个候选攻击 Action，其发生的可能性大于计算其他候选攻击发生的可能性并且其匹配度大于 a，则跳转到 4；如果候选攻击集合中不存在一个候选攻击和当前发生的攻击行为相匹配，则跳转到 5。

4) 添加 Action 到攻击模型 M_j 的 $S_{d,j}$ 中，完成 $S^C=S^C-\{Action\}$，然后计算 Action 发生后可能发生新的候选攻击集合 *CandiAttackSet* 并根据其元信息进行实例化，使得 $S^C=S^C_{dd}\cup CandiAttackSet$，新候选攻击集合的时间戳 Ctimestamp 为当前的时间，跳转到 2。

5)重建新的攻击模型 M，将该 *Alert* 所代表的攻击动作做为模型 M 的 S_d，计算 S_c，并将其加入到跳转 1。

3.2 候选攻击集合的计算

每种攻击的发生都需要前提条件[13]。如果该前提条件被攻击者所掌握，则攻击者有很大的可能性会发动该攻击。但由于攻击的多样性，相同的前提条件可能会导致多种攻击有发生的可能性[15]。为了计算基于当前入侵者的知识而可能发生的攻击，定义了一决策表。该决策表的属性集 A 满足以下条件：$A=C\cup D$，$C\cap D=\varnothing$，C 称为条件属性集，D 称为决策属性集。$C=(Existssnmp, Esistsip,\cdots)$，而 $D=(AttackType)$。

假设当前攻击者已经获得的知识 HK=$\{know_1,know_2,\cdots,know_m\}$，而攻击者发动攻击 Attack_i 所需要的知识为 $AK_i=(knowledge_{i,1},knowledge_{i,2},\cdots\cdots,knowledge_{i,n})$，则

$POS_{HK}(AttackType)=\{\text{Attack}_i\}\ AK_i\subseteq HK$

$UPBND_{HK}(AttackType)=\{\text{Attack}_i\}\ HK\subset AK_i\ \ HK\neq AK_i$

$DownBND_{HK}(\text{AttackType})=\{\text{Attack}_i\}\ HK\cap AK_i\neq\Phi\ \exists yy\in HKy\notin AK_i$

$NEG_{HK}(AttackType)\ HK\cap AK_i=\Phi$

从上述定义可知，由于假设攻击者攻击发动的每一步都是有目的的活动，其发生的可能性可排序为：$POS_{HK}(AttackType)>UPBND_{HK}(AttackType)>DownBND_{HK}(AttackType)>NEG_{HK}(AttackType)$

在进行攻击场景重构的过程中，可以通过它选择出最可能发生的攻击场景集合。由于 $NEG_{HK}(AttackType)$ 的 $HK\cap AK_i=\Phi$，因此可以认为 $NEG_{HK}(AttackType)$ 内的攻击类型都不是前一攻击的后序动作，所以

$\text{AttCandidateSet}=POS_{HK}(AttackType)\cup UPBND_{HK}(AttackType)\cup DownBND_{HK}(AttackType)=\{\text{AttCan}_1,\cdots,\text{AttCan}_n\}$

3.3 报警事件的可信性计算

假设网络中有 m 个安全设备，设备 $s_k(1\leqslant k\leqslant K)$ 可以对攻击 $Attack_i(1\leqslant i\leqslant M)$ 进行检测。当攻击 $Attack_i$ 在网络地址为 Src_Ip 和 Dst_Ip 两台主机之间发生的时候，设备 s_k 会产生相应的报警信息，$Alert_i=(\text{Attacktype}_i,\text{Src\_Ip},\text{Src\_Port},\text{Drc\_Ip},\text{Dst\_port},\text{Time\_stamp})$，则在地址为 Src_Ip 和 Dst_Ip 两台主机之间，安全设备 s_k 检测到发生的攻击为 $Attack_i$，而实际发生的攻击为 $Attack_j$ 的概率为 $p_k(Attack_j|Attack_i)$，即 $p_k(Alert_j|Alert_i)$。假设当前安全设备集产生的报警事件集合 AS 为 $\{Alert_1,Alert_2,\cdots,Alert_{k'}\}$，则可以计算每种报警信息 $Alert_i(1\leqslant i\leqslant k',k'\leqslant k)$ 的可信度 $Bel(Alert)$，其中 *Alert* 的取值可为报警事件集 AS 的任一元素)：

$$Bel(Alert)=Bel(Alert|s_1,\cdots,s_k)=p(Alert|Alert_1,\cdots,Alert_{k'})=\frac{p(Alert_1,\cdots,Alert_k|Alert)p(Alert)}{p(Alert_1,\cdots,Alert_{k'})}=\frac{\prod_{i=1}^{k'}p(Alert_k|Alert)p(Alert)}{\prod_{i=1}^{k'}p(Alert_k)}=\frac{\prod_{i=1}^{k'}p(Alert_k|Alert)}{\prod_{i=1}^{k'}p(Alert_k)}p(Alert)$$

$$=p(Alert)\frac{\prod_{i=1}^{k'}p(Alert|Alert_k)}{\prod_{i=1}^{k'}p(Alert)}$$

$$Bel(Alert)=p(Alert)\frac{\prod_{i=1}^{k'}p(Alert|Alert_k)}{\prod_{i=1}^{k'}p(Alert)}=\frac{p(Alert)}{\prod_{i=1}^{k'}p(Alert)}$$

$$\prod_{i=1}^{k'}p(Alert|Alert_k)=\lambda\prod_{i=1}^{k'}p(Alert|Alert_k)$$

$$Bel(Alert)\sim\prod_{i=1}^{k'}p(Alert|Alert_k)$$

对报警事件集 AS 中的元素按照其 *Bel* 值的大小进行排序，选择最可能发生的 L 个报警事件参与进一步的关联操作，其中 $L\leqslant k''$。在此，需要进一步说明的是，其中 L 的值不是常量，L 的大小取决于当把报警事件集 AS 中的元素的 *Bel* 值从大到小映射到一二维坐标空间，其值可拟合一曲线，取该曲线的切线的斜率首次变化比较剧烈的点做为分界点，该点前面的 L 个报警事件将参与进一步的场景重构操作。

4 试验

4.1 数据集

DARPA 在 2000 年提供了两个可用于测试攻击场景重构的基准测试数据集[8]，即 LLDOS1.0 和 LLDOS2.0，其中 LLDOS1.0 包含一个由 5 个攻击步骤构成的 DDOS 攻击场

景，该 5 个攻击步骤分别为：Ipsweep、probe、Breakin、安装 Mstream 木马软件和发动 DDOS 攻击，而 LLDOS2.0 包含的攻击场景和 LLDOS1.0 类似，只是更加复杂。每个数据集都包括分别从 DMZ 和内网两个区内获取的网络数据流。我们利用这 4 个数据子集，设计了 4 个试验去验证算法的有效性。

4.2 试验环境

试验过程中，我们利用 TCPReplay 重播 LLDOS1.0 和 LLDOS2.0 两个测试数据集中所包含的 4 个数据子集，并同时用 ISS 的 RealSecure Network Sensor 6.5、snort 1.8 和 bro 0.8 去获取重播的数据报文，产生报警事件集合，然后利用该事件集去验证算法的有效性。在此需要说明的是，RealSecure Network Sensor 6.5 的安全策略为 Maximum_Coverage policy 策略配置。本文所设计的试验环境与文[13]相似，唯一的区别是本文中选用的 RealSecure Network Sensor 的版本是 6.5，而文[13]中为 6.0 的版本。

4.3 参数计算

在对每个报警信息进行可信性计算的时候，需要先验知识 $p(Alert)$、$p(Alert_i \mid Alert_i)$。对此的计算采用以下方式：首先下载 DARPA1998 的训练数据集合，然后通过该数据集合利用安全设备 S_k 建立以下矩阵：

$$PT_k=\begin{pmatrix} n_{11}^{(k)} & n_{12}^{(k)} & \cdots & n_{1M}^{(k)} & n_{1(M+1)}^{(k)} \\ n_{21}^{k} & n_{22}^{(k)} & \cdots & n_{2M}^{(k)} & n_{2(M+1)}^{(k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ n_{M1}^{(k)} & n_{M2}^{(k)} & \cdots & n_{MM}^{(k)} & n_{M(M+1)}^{(k)} \end{pmatrix}$$

对于矩阵 PT_k，其第 i 行对应着攻击 $Attack_i$，第 j 列对应着报警事件 $Alert_j$。因此，矩阵里面的元素 $n_{ij}^{(k)}$ 表示安全设备 S_k 在攻击 $Attack_i$ 发生的时候产生的报警事件为 $Alert_j$ 的数目。根据此矩阵，可以计算出攻击 $Attack_i$ 的个数 $n_i=\sum_{j=1}^{M+1} n_{ij}^{(k)}$，$i=1,\cdots,M$，产生报警信息 $Alert_j$ 的数目为 $n_j=\sum_{i=1}^{M} n_{ij}^{(k)}$，$j=1,\cdots,M+1$，则 $p(Alert_i \mid Alert_j)=\frac{n_{ij}^{(k)}}{n_i^{(k)}}$，同样可以很容易计算出 $p(Alert)$。

4.4 试验结果及其分析

首先利用 DARPA 数据集来验证算法的有效性，如图 2 和图 3 所示，分别是利用算法从 LLDOS1.0 和 LLDOS2.0 的两个数据集所产生的报警事件重构出的的攻击场景图。

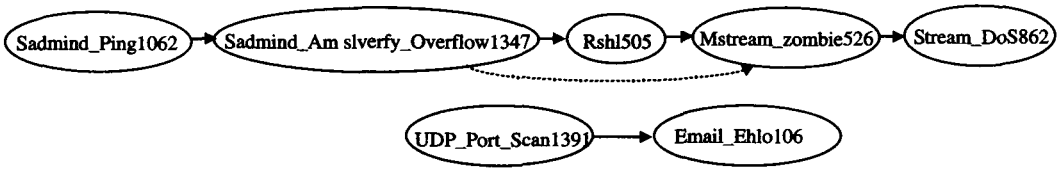

图 2 攻击场景图

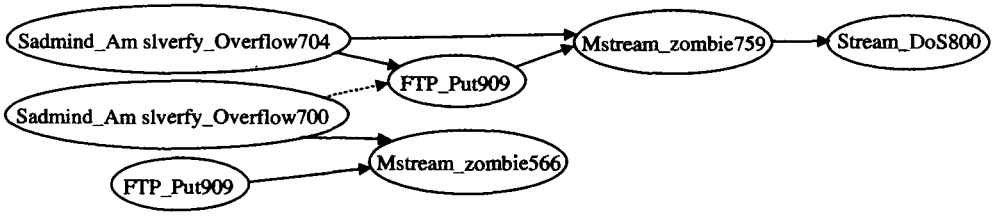

图 3 攻击场景图

从图 3 可以看出，LLDOS1.0 和 LLDOS2.0 中所蕴涵的攻击过程通过此算法已经被完整地重构出来。同时可清晰地看出攻击者在攻击过程中所利用的攻击手段、攻击策略和攻击目标。图 3 是一个攻击过程的高度聚和图。需要说明的是，图中的虚线部分表示攻击者可能使用的攻击路径。与文[13]相比，Email Almail Overflow 和 FTP Syst 没有被关联到图 2 的场景图中，其性能有了一定程度的提高。但在关联结果中，也产生了一些攻击场景噪声，如图 2 中的第二个攻击场景图。这是本工作一个未来改进的方向。

除了验证文中所提出的算法在场景重构方面的性能，还验证了该算法在对报警事件约减方面的性能，结果如表 1 所示。

表 1 验证结果

DataSet		observable attacks	Tool	# Alerts	# detected attacks	Detection Rate	# true alerts	False Alert Rate
LLDOS 1.0	DMZ	87	RealSecure	890	49	56.32	57	93.6
		43	Ours	53	30	69.7	49	7.55
	Inside	60	RealSecure	920	37	61.67	44	95.21
		35	Ours	42	22	62.86	40	4.6
LLDOS2.0	DMZ	7	RealSecure	425	4	57.14	6	98.59
		5	Ours	7	3	60	5	28.57
	Inside	15	RealSecure	489	12	80.00	16	96.73
		8	Ours	9	7	87.5	8	11.11

在表1中，主要统计了与算法有关的以下统计指标：

检测率(Detection Rate)＝正确报告的攻击数/可以被观测到的攻数；

误报率(False Alert Rate)＝1－正确的报警数/所有产生的报警数。

为了计算以上统计指标，需要根据DARPA提供的文档计算数据集和算法的结果集中所包含的攻击数和误报数目。对攻击数目的统计是比较困难的，因为到现在为止，还没有一个统一的视角去看待一次攻击的发生。本文采用文[12]中描述的方法，即整个攻击过程的第一个阶段和最后一个阶段虽然包含很多的数据报文，但只分别记做一个攻击。而对于其余阶段的每个动作，如telnet等，即使不一定是一种攻击，但认为其有可能是参与某攻击的一部分，也将其做为一个攻击的发生。攻击的数目如表1所示。而对于误报的数目，可以根据DARPA所提供的文档很容易计算出来。表1总结了整个试验的试验结果。从计算结果可以看出，该算法在减少误报率方面取得了比较好的性能。而对于检测率，从表1可以看出，也有了很大程度的提高。但实际上，该值的变化仅反映出在本环境中该算法对检测率的影响，而对于是否在任何环境中都能提高检测率，需要做进一步的验证和分析，主要原因是检测率的提高与否依赖于参与的安全设备本身的性能以及它们之间的差异性，即单个安全设备的检测率越高，它们之间的差异性越大，其检测率有可能比任何一个单个设备的检测率都高。否则，有可能相反，此理论类似于文[25]。

5 相关工作

和文[13]的方法相比，该文主要使用攻击的前提和攻击的后果来进行关联，认为前一个攻击的后果是后一个攻击的前提，通过这样的关系，将两个攻击联系起来。这种方法的弱点是：虽然能将具有紧密联系的攻击联系起来，但不能对不具有紧密联系的攻击方法联系起来。因为攻击者攻击时，会利用多种攻击方法，这些方法之间不一定具有必然的前因后果联系，所以有可能不能构建攻击者的完整的攻击行为。

目前已提出许多方法进行报警关联，建立攻击场景。主要有3类方法：(1)利用报警属性之间的相似性进行关联[2,4,19,20]；(2)利用事先已知的攻击场景进行关联分析，即事先分析、建立攻击场景库[9,21]；(3)不需事先建立攻击场景，利用已知攻击的前提条件和后果进行关联[4,13]，即只根据因果关系，将有直接因果联系的攻击关联起来，组成攻击场景。这3种方法各有优缺点：第1种方法比较简单、实用，但只能关联一些简单的事件；第2种方法是不易建立已知攻击场景库，不能覆盖全部的已知攻击模式，不能发现新的攻击场景；第3种方法的优点是不需事先建立攻击场景，只要根据攻击的前提条件和后果关联相关的攻击事件，且能发现新的攻击场景；缺点是很多攻击场景的攻击之间没有明显的因果关系，无法通过此方法构造出来，且事先也需要建立攻击信息库，确定每种攻击的前提条件和后果关系。另外，该方法在建立模式时，空间复杂度比较高，容易引起状态空间的膨胀。根据以上分析，第1，3种方法的分析结果只是提供了一些简单的关联分析，不能有效提供攻击者的真正意图和方法；第2种方法仍然是最有效的方法，但存在攻击场景不易描述、构造，不易发现新的攻击场景的问题，影响了该方法的有效性。

攻击场景重构的重点是描述攻击场景的方法，以及这些方法对攻击场景重构的支持。描述攻击模型的方法很多，有攻击树[22]、攻击图等方法。攻击树分层次结构描述攻击，规定了攻击的先后顺序，易于理解，同时有利于不同的专家并行处理分支树的内容，能并行处理攻击分支；其缺点是无法提供描述攻击前提条件的方法，在同一个节点中不易区分攻击的动作和结果，且其结构采用AND/OR的方法，不易扩展。但Petri网是一个很好的描述攻击的方法，不仅有图形的直观性、结构的层次性，还有一套理论方法支持系统的性质分析和品质分析。目前已有将Petri网用于攻击测试[23]和攻击检测[24]的应用。它们的应用说明petri网能很好地描述系统攻击场景，便于在不同的对象之间交换信息。但它们只是利用petri网描述攻击步骤，主要用于在用户之间交换攻击步骤信息，还不能直接用于攻击场景重构。

结束语 本文利用贝叶斯规则对多个安全设备产生的报警信息进行融合，生成了可信的报警信息集合。在此基础上完成了攻击场景的重构工作，从而减少了误报对关联算法的影响，提高了关联算法的健壮性和扩展性。另外，该方法可以使报警事件约减和场景重构同时进行，实现了对报警事件的在线分析功能，提供了存在于攻击场景的潜在攻击路径，弥补了原有算法的不足。试验结果表明，该算法在场景重构方面和报警事件约减方面都表现了良好的特性。本算法仅仅进行了离线状态下的数据验证，还需要进一步在实际环境中验证该算法的性能。

参 考 文 献

1 Krogh A, Vedelsby J. Neural network ensembles, cross validation, and active learning. In: Tesauro G, Touretzky D S, Leen T K, eds. Advances in Neural Information Processing Systems 7, Cambridge, MA: MIT Press, 1995. 231～238

2 Valdes A, Skinner K. Probabilistic alert correlation. In: Proc. of the 4th International Symposium on Recent Advances in Intrusion Detection(RAID), October 2001

3 Curry D, Debar H. Intrusion Detection Message Exchange Format. http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-10.txt. August 2003

4 Cuppens F, Miège A. Alert Correlation in a Cooperative Intrusion Detection Framework. In: 2002 IEEE Symposium on Security and Privacy, May 2002

5 Cuppens, Autrel F, Miege A, et al. Correlation in an intrusion detection process. Internet Security Communication Workshop(SECI'02), Sep. 2002

6 Cuppens F. Managing Alerts in a Multi-Intrusion Detection Environment. In: 17th Annual Computer Security Applications Conference, New-Orleans, USA, December 2001

7 Jiang G, Cybenko G. Temporal and Spatial Distributed Event Correlation for Network Security. In: 2004 American Control Conference, Boston, June 30～July 3

8 Debar H, Wespi A. Aggregration and Correlation of Intrusion-Detection Alerts. In: Proceedings of the 4th International Symposium on Recent Advances in Intrusion detection(RAID), 2001

9 Lincoln Lab, MIT. DARPA 2000 intrusion detection evaluation datasets. http://ideval.ll.mit.edu/2000/index.html, 2000

10 Haines J, Ryder D K, Tinnel L, et al. Validation of Sensor Alert Corre-lators. IEEE Security and Privacy, 2003, 1(1): 46～56

11 Sheyner O, Haines J, Jha S, et al. Automated generation and analysis of attack graphs. In: Proceedings of the 2002 IEEE Symposium on Security and Privacy, Oakland, CA, May 2002

12 Porras P A, Fong M W, Valdes A. A Mission-Impact-Based approach to INFOSEC alarm correlation. In: Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection(RAID), October 2002

13 Ning P, Cui Y, Reeves D S. Constructing attack scenarios through correlation of intrusion alerts. In: 9th ACM Conference on Computer and Communications Security, November 2002

14 Benferhat S, Autrel F, Cuppens F. Enhanced Correlation in an Intrusion Detection Process. Second International Workshop Mathematical Methods, Models and Architectures for Computer Networks Security, St Petersburg, Russia, September 2003

15 Templeton S J, Levitt K. A requires/provides model for computer attacks. In: Proceedings of the 2000 Workshop on New Security Paradigms, 2001. 31～38

16 Qin X, Lee W. Statistical causality analysis of INFOSEC alert data. In: Proceedings of the 6th International Symposium on Recent

Advances in Intrusion Detection(RAID 2003), Pittsburgh, PA, September 2003
17 Qin X, Lee W. Discovering novel attack strategies from INFOSEC alerts. In: Proceedings of the 9th European Symposium on Research in Computer Security, Sophia Antipolis, France, September 2004
18 Qin Xinzhou, Lee Wenke. Attack Plan Recognition and Prediction Using Causal Networks. ACSAC 2004: 370～379
19 Staniford S, Hoagland J, McAlerney J. Practical automated detection of stealthy portscans. Journal of Computer Security, 2002, 10(1-2): 105～136
20 Dain O, Cunningham R. Building scenarios from a heterogeneous alert stream. In: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 2001. 231～235
21 Dain O, Cunningham R. Fusing a heterogeneous alert stream into scenarios. In: Proceedings of the 2001 ACM Workshop on Data Mining for Security Applications, Nov. 2001. 1～13
22 Schneier B. Attack Trees. Dr Dobb's Journal of Software Tools, 1999(12): 21～29
23 McDermott. Attack Net Penetration Testing. The 2000 New Security Paradigms Workshop(Ballycotton, County Cork, Ireland, Sept. 2000). In: ACM SIGSAC, ACM Press, 2000. 15～22
24 Helmer G, Wong J, Slagell M, et al. Software Fault Tree and Colored Petri Net Based Specification, Design and Implementation of Agent-Based Intrusion Detection Systems
25 Breiman L. Bagging Predictors. Machine Learning, 1996, 24(2): 123～140

(上接第 99 页)

C 节点加入 节点加入分两种情况：第一种情况是当一个节点第一次入网。第二种是一个节点脱离原簇加入另一个簇的情况。前者，由于节点没有信任值证书或者推荐证书，簇首不得不从头开始对该节点的信任值进行评估。在第二种情况，脱离原簇的节点向新簇首出示在原簇获得的信任值证书和推荐证书。依据这些证书，新簇簇首鉴别和设置新加入的节点的初始信任值而不需要其经验值。过程如下：首先，节点广播"Hello"探测消息，一些收到消息的簇首向该节点回复响应信息。响应信息中包括簇首所在簇的成员数量。其次，收到簇首响应信息的节点再向想要加入的簇的簇首发送加入消息，如下所示。

Joim Message:

M(node1's id, cluster head's id, previous cluster head's id, T_Certificate, R_Certificates, "join message")

若加入节点的邻居节点中簇首的数目超过两个，则选择簇成员最多的簇加入。第三，簇首收到请求加入的消息后，它根据请求加入节点原所在簇为其颁发的信任值证书评估该节点的信任值。如果申请加入的节点在一跳范围内没有找到可以申请的簇首就扩大范围搜索两跳的，若还没有找到，就只能和相邻的节点重建一个新簇。

D 节点离开 当一个节点离开原簇时向原簇首发送离开消息，原簇首收到后删除该节点的相关信息。

3 应用分析

此信任方案可应用于解决针对移动自组网的各种攻击引起的安全问题和安全路由的设计。

3.1 安全路由

应用 CBTES 方案，一个节点收到的路由请求的附加信息包括 T_Certificate, R_Certificates 和节点本身的地址。信息源在收到路由回复数据包后检查中间节点的信任值。如果中间有些节点的信任值较低，则信息源节点放弃这条路由，重新广播路由请求包来寻找别的路径。

3.2 其它安全问题

· 消息伪造攻击：本方案采用 Rakesh 不对称加密法[5]，同时在消息中绑定数字签名和发送者的公钥。这样接受者就可以检测公钥是否是发送者的，从而断定消息是否伪造。

· 黑洞攻击：攻击者在某节点的路由请求和路由回复过程中宣称自己拥有到目的节点的最短路由，这样该节点会选择其所宣称的路由，从而将数据包发向攻击节点，攻击节点截取数据包不再转发，在网络中形成一个吸收数据的"黑洞"。在本方案中，恶意节点的信任值会非常低，恶意节点宣称的路由将被放弃，从而保证数据的安全。

· 自私攻击：由于移动自组网的特殊性，网络中的部分节点可能会由于资源能量、计算能量等原因不愿意承担其它节点的转发任务而产生自私性攻击。在本方案中，自私节点由于数据转发率低导致其不可能有一个较高的信任值。通过不提供给低信任值节点数据包的方法，网络可以促进合作和减少自私节点。

结论 本文提出了一个针对移动自组网的新型信任评估方案，即基于分簇的信任评估方案。该方案可以解决移动自组网中现存的许多安全问题。依据该方案，移动自组网内任何一个节点都可以凭借簇首签发的信任值证明书对另一个陌生节点进行信任评估，从而使得每个节点均可以通过一种安全的方式和其它以前从未与之有过通信连接的节点进行通信。同时，由于网络节点不需要收集和存储移动自组网内所有其它节点的信任值的经验数据，大大减少了信任评估过程所需的资源开销。

参 考 文 献

1 Deng H, Li Wei. Agrawal D P. Routing Security in Wireless Ad Hoc Networks. IEEE Commun. Mag., 2002, 40(10): 70～75
2 Yan Z, Zhang P, Virtanen T. Trust Evaluation Based Security Solution in Ad Hoc Networks: [Technical Report]. Nokia Research Center, Helsinki, Finland, Oct. 2003
3 Pirzada A A, McDonald C. Establishing Trust In Pure Ad-hoc Networks. In: Proc. Australasian Computer Science Conf., Jan. 2004. 47～54
4 Gerla M, Tsai J T C. Multicluster, Mobile, Multimedia, Radio Network [J]. Wireless Networks, 1995, 1(3): 255～265
5 Sarela M, Hietalahti M. Security Topics and Mobility Management in Hierarchical Ad Hoc Networks: A Literature Survey: [Interim Report of Project Samoyed]. Helsinki Univ. of Technology, Apr. 2004
6 Bechler M, et al. A Cluster-Based Security Architecture for Ad Hoc Networks. In: Proc. IEEE INFOCOM, 2004, 4: 2393～2403
7 Park Chan-Il, Lee Y H, Yoon H, Choi D S, Jin S H. Cluster-Based Trust Evaluation in Ad Hoc Networks. In: Proc. Int'l Conf. Advanced Communication Technology, 4C-03, Feb. 2005
8 Basagni S. Distributed Clustering for Ad Hoc. Networks. In: Proc. Int'l Symp. Parallel Architectures, Algorithms, and Networks, 1999. 310～315
9 Bobba R B, et al. Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks: [Technical Report, TR2002-44]. Univ. of Maryland, May 2002
10 Marsh S P. Formalizing Trust as a Computational Concept: [Ph. D. Thesis]. Dept. of Mathematics and Computer Science, Univ. of Stirling, 1994