Journal of Computer Applications
计算机应用,2014,34(1):108 - 112
ISSN 1001-9081
CODEN JYIIDU
2014-01-10
http://www.joca.cn

文章编号:1001-9081(2014)01-0108-05
doi:10.11772/j.issn.1001-9081.2014.01.0108

基于攻击图与报警相似性的混合报警关联模型

朱梦影,徐　蕾*
(沈阳航空航天大学 计算机学院,沈阳 110136)
(*通信作者电子邮箱 xulei@sau.edu.cn)

摘　要:为了揭示入侵检测系统所生成的报警数据之间的关联关系和重构入侵攻击场景,提出了一种基于攻击图与报警数据相似性分析的混合报警关联模型。该模型结合攻击图和报警数据分析的优点,首先根据入侵攻击的先验知识定义初始攻击图,描述报警数据间的因果关联关系,再利用报警数据的相似性分析修正初始攻击图的部分缺陷,进而实现报警关联。实验结果表明,混合关联模型能够较好地恢复攻击场景,并能够完全修复攻击图中单个攻击步骤的缺失。

关键词:报警关联;入侵场景;攻击图;报警相似性;关联模型
中图分类号:TP393.08　　**文献标志码**:A

Hybrid model of alert correlation based on attack graph and alert similarity

ZHU Mengying, XU Lei*
(*School of Computer, Shenyang Aerospace University, Shenyang Liaoning* 110136, *China*)

Abstract: In order to reveal logic attack strategy information from alarms generated by intrusion detection system and reconstruct attack scenario, a hybrid model of alarm correlation was proposed, which was based on attack graph and alert similarity analysis. This model combined the advantages of attack graph and alert data analysis. First of all, it described the causal relationship between alarms, according to the initial attack graph defined by the prior knowledge of intrusion attack. Afterwards, it used the similarity analysis of the alert data to repair the defects of the initial attack graph. And then it implemented alert correlation. The experimental results show that the model can not only recover attack scenario but also be able to fully repair the attack graph in the absence of a single attack step.

Key words: alert correlation; intrusion scenario; attack graph; alert similarity; correlation model

0　引言

目前网络入侵的手段更加复杂化,入侵攻击通常是经过多步骤协同工作完成的;入侵检测系统(Intrusion Detection System, IDS)在不断增强入侵检测能力的同时仍然存在误报率高、报警数据量过多以及报警语义弱等不足[1]。如何自动地从IDS的低层报警中,剔除冗余和错误的报警,发现报警之间的关联关系,分辨出完整的入侵攻击过程,成为提高IDS可用性的首要问题。

报警关联技术已经成为IDS领域的研究热点之一。根据报警关联是否使用先验条件可将报警关联方法分为两类。基于先验知识的方法,如典型的TIAA[2]方法是将攻击表示为攻击的前提和后果,如果攻击A的后果匹配攻击B的前提,则B被认为是A的后续攻击步骤。这个方法需要建立包含攻击前提和后果的知识库,利用匹配的方法完成报警的关联过程。在此基础上,Debar[3]提出的基于攻击图的报警关联方法是利用规则将各报警连接成图,利用图搜索完成报警信息关联。这类方法需要预先定义攻击的前提与后果关系,定义阶段需已知攻击的专门知识和手工操作,导致此类方法的实时性和拓展性受到制约。

不需要先验知识的报警关联方法弥补了上述不足,Valdes等[4]提出的基于报警相似度的关联方法是具有代表性的方法之一,方法利用报警属性相似度的加权和得到报警相似度,对相似度大于给定阈值的报警做关联。Ren等[5]提出了基于贝叶斯公式的特征选择模型,用于计算报警的关联概率。此类报警关联方法的优点是不受先验知识的约束,能够发现一些新的攻击;缺点是不易找出多步攻击报警之间真正的因果关系,只能发现统计上的关联情况。

Ahmadinejad等[6]提出的利用攻击图和报警相似度做报警关联的混合模型互补了两类方法的不足。此模型在报警相似度向量[7]或初始攻击图定义不完善时,会导致较多的错误关联结果。本文提出的混合关联模型基于报警数据的相似性分析修补初始攻击图定义的缺陷。实验结果表明,模型较好地解决了报警数据和已知的攻击步骤不匹配而导致的报警数据关联失败问题,能够实现部分语义不明确报警的数据归类。

1　混合报警关联模型

混合报警关联模型是利用攻击图和报警数据相似性分析的方法进行报警数据关联。

1.1　模型结构

模型的输入是多个IDS产生的报警数据,结构如图1所示。

收稿日期:2013-07-01;**修回日期**:2013-09-26。

作者简介:朱梦影(1989 -),女,河南许昌人,硕士研究生,主要研究方向:网络与信息安全;　徐蕾(1959 -),女,上海人,教授,主要研究方向:网络与信息安全。

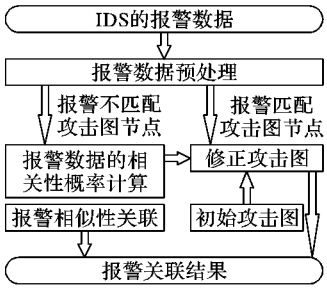

图 1　混合报警关联模型结构

模型将多个 IDS 的报警数据按照入侵检测信息交换格式(Intrusion Detection Message Exchange Format, IDMEF)[8]构成 9 个属性的多元组(senserID, src_ip, dst_ip, src_port, dst_port, timestamp, type, sign, timeintes)。其中:senserID 是报警序列号,src_ip 和 dst_ip 是报警的源和目的 IP 地址,src_port 和 dst_port 是报警的源和目的端口,timestamp 是报警触发的时刻,type 表示报警所属的攻击类别,sign 表示报警名称,timeintes 表示报警检测时间。

模型首先对报警数据进行预处理,报警预处理主要去除 IDS 报警数据中的周期性数据和重复性数据。攻击触发的报警具有突发性,其报警时间是不确定的,具有随机性的特点[9];报警数据中出现的周期性报警通常是由于一些固定事件引起的,如网络定期检查等;模型利用傅里叶变换的方法找出周期性的报警,从而消除 IDS 所产生周期性的误报警。IDS 会在短时间内产生大量的重复报警[10],在报警数据预处理阶段使用基于动态滞留时间与多级聚合粒度的自适应算法去除原始报警中的重复报警。

预处理后的报警数据用于报警的相关性概率计算,为后续报警关联提供依据。

若报警数据在攻击图中可以直接匹配原子攻击节点,则按照攻击图中原子攻击节点之间的连接关系进行报警数据关联。若报警在攻击图匹配时缺失部分前提报警,模型中假设虚拟前提报警并在图中利用深度优先搜索查找其间接的前提报警;如果缺失的前提报警数太多,则利用报警相似性分析做补充关联。最终得到报警关联结果。

若报警在攻击图中不能直接匹配原子攻击节点,模型计算报警与已知报警的关联概率,并以此为依据分析报警的相似关系,利用相似报警得出此报警与攻击图中原子攻击的映射或关联关系并更新攻击图。

1.2　基于攻击图的报警关联

本文采用属性攻击图[11]识别报警数据之间的关联关系。属性攻击图由两种节点构成:一种表示攻击者利用系统或网络的某个漏洞进行的单次攻击,称为原子攻击节点;另一种表示原子攻击前和实施攻击后被攻击机器的系统状态及其改变情况,称为系统属性节点。原子攻击节点与属性节点使用前提边和后果边连接,所有通过前提边与原子攻击节点相连的属性节点都满足时,该原子攻击才可被执行,从而使通过结果边与该原子攻击相连的属性都被满足。

利用攻击图中原子攻击的前、后序关系可得到攻击所对应的报警之间的关联关系,报警关联可用报警图表示。报警可以认为是攻击图中原子攻击的实例化,带有攻击的位置特征,因此在攻击图的原子攻击和报警图的对应报警之间建立映射关系。在报警图中,报警名、报警的源和目的 IP 地址都相同的报警可看作无差别的报警,将这些报警按照出现时间增序排列,用 name(sip,dip)表示,其中 name 为报警名、sip 和 dip 为报警的源和目的 IP 地址;攻击图中的原子攻击节点可得到报警图中的多个报警节点。攻击图中的属性节点可转换为报警图中某机器的系统或网络属性,用 attr_name(aip)表示,其中 attr_name 为属性名,aip 是机器 IP 地址。报警是由攻击产生的,而攻击与被攻击对象某些系统属性或漏洞相关,因此报警的源 IP 或目的 IP 地址应该和相连的属性节点的地址相一致,这种地址的对应关系由报警和属性节点连接边上的地址传递函数表示。攻击图演变的报警图如图 2 所示。

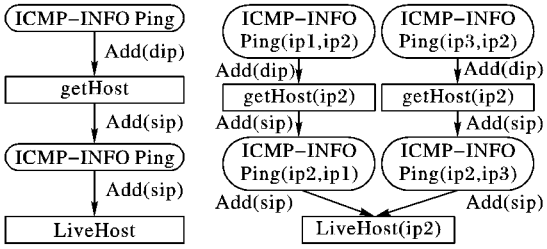

图 2　由攻击图构造报警图

若报警的报警名与原子攻击的名称相同,则直接在两者之间建立映射关系,若报警名与攻击图中原子攻击的名字都不相同,则利用下节给出的报警相似分析的方法建立报警与所对应攻击节点之间的映射关系。报警数据 M 加入报警图的方法如下:

1)M 的报警名、源 IP 和目的 IP 与报警图中节点 U 的对应参数相同,将 M 加入该节点的报警序列,在 M 加入 U 之前若 U 被标记是虚拟报警节点(虚拟报警节点在第 2)步中产生和标记),加入 M 后 U 及其结果属性节点都去掉虚拟标记。

2)在报警图中不存在与 M 的上述参数相同的节点,但 M 的报警名与攻击图的原子攻击节点 M' 存在映射关系,则在报警图中新建包含 M 的报警节点 U,并生成 U 的全部结果属性节点。若 M' 不是攻击图的根节点,按照攻击图中 M' 节点的前提属性及其地址传递关系在报警图中查找与报警 M 满足地址关系的前提属性节点,若存在,在 U 和前提属性节点之间建立前提边,若在报警图中找不到 U 的前提属性和相应的前提报警,说明报警 M 在攻击图中前提攻击步骤对应的报警可能丢失,则从 M' 开始,按照深度优先的方法在攻击图中查找 M' 的前提攻击对应的报警在报警图中是否出现,若在限定的深度阈值范围内找到相应的前提报警节点 V,在 U 和 V 之间按照攻击图中边的连接关系构造一条路径,路径中 U 与 V 之间的节点标记为虚拟的报警和属性节点。

3)M 与攻击图中的任何原子攻击节点不存在映射关系,或者在 2)中没有找到 M 的前提属性或前提报警节点,则利用相似报警的计算方法得到 M 的相似报警或者相似的前提报警,M 根据相似报警建立报警关联关系,详细的方法说明见 1.3 节。

1.3　基于报警相似性分析的报警关联

部分报警在攻击图中找不到与原子攻击的映射关系,利用报警相似性分析可以间接地获得报警与原子攻击之间的对应关系进而实现报警关联。

报警的相似性分析采用条件概率进行计算,分析报警相似性时,以报警名区分不同的报警,报警类 $A = \{a_1, a_2, \cdots,$

$a_n\}$ 表示报警中属性 sign(报警名) 的值为 A 的报警集合。当名为 A 的报警出现时,与 A 相关的名为 B 的报警已经出现的概率可以利用条件概率公式 $P(B|A)=P(A\wedge B)/P(A)$ 计算。

不同的报警属性在报警相似性计算中其重要程度是不同的。对于不同类型的报警,在报警相似性计算中,根据属性的重要程度赋予不同的权值并忽略作用小或无关的属性,将增加报警相似性计算的准确率和减少计算量。报警相似性分析及计算的步骤如下:

1) 计算报警相关性概率,在计算中得出对报警相似性计算起重要作用的报警属性,得出报警相似计算的重要属性集。

2) 根据上一步得出的重要属性集,建立报警关联关系并补充攻击图。

1.3.1 计算报警相似性的重要属性集

首先计算报警属性对报警相似性计算的影响程度。设报警属性集为 $\{f_1,f_2,\cdots,f_j,\cdots\}$,一个报警 a 的 f_j 值写成 $a[f_j]$,报警 a(报警集合 A) 的 f_j 值域记为 $dom(a,f_j)$($dom(A,f_j)$);报警数据的 f_j 值域写成 $dom(f_j)$,则有 $dom(A,f_j)\subseteq dom(f_j)$。利用条件概率公式计算报警属性 f 在两个不同名的报警类 (A,B) 的相似性计算中的重要程度。也就是计算报警 $a\in A$ 出现后,报警 $b\in B$ 已经出现且其 f 属性值等于 $a[f]$ 的概率;即计算 $P(B|A\wedge dom(A,f)\subseteq dom(B,f))$(写成 $P(B_f|A_f)$)。

假设报警类 $A=\{a_1,a_2,\cdots,a_n\}$,$B=\{b_1,b_2,\cdots,b_m\}$,将 A 中的报警按 f 属性值分组,分组后 $A=\{A_1,A_2,\cdots,A_k\}$,即 $A_i=\{a_{i,1},a_{i,2},\cdots,a_{i,j},\cdots\}$ 中所有报警的 f 属性值相同。$P(B_f|A_f)$ 的计算过程如下:

1) 设集合 $AF=\varnothing$,$ABF=\varnothing$。

2) 取 $A_i\in A$,A_i 的 f 属性值为 v_i,若 $v_i\in dom(B,f)$,则 $AF=AF\cup A_i$,将 A_i 集合报警中最小的时间戳存入 *firstTime*。

3) 将满足下列条件的报警 $b\in B$ 加入集合 ABF:

①$b[f]=v_i$;

②b 的时间戳 $t_b<firstTime$ 且 $firstTime-t_b<timePeriod$。

4) 重复 2) ~ 3),直至处理完 A 中所有序列。

计算概率

$$P(B_f|A_f)=\frac{P(A\wedge B\wedge dom(A,f)=dom(B,f))}{P(A|dom(A,f)\subseteq dom(B,f)}=\frac{|ABF|}{|AF|}$$

计算中使用的时间阈值 *timePeriod* 是限定在报警 a 之前出现的报警 b 的时间范围。理论上时间阈值大,能够找到前提关系发展缓慢的攻击,但分析困难。*timePeriod* 的值是根据系统与攻击的特点合理设定的。

定义属性重要性判断阈值 T,若 $P(B_f|A_f)>T$,认为两报警类 (A,B) 计算相似性时,f 是计算的重要属性。

利用贪心选择算法依据 $P(B_f|A_f)$ 的计算方法可得到 (A,B) 报警相似性计算的重要属性集。贪心选择算法如下:

1) 针对两报警类 (A,B) 的属性集 $F=\{f_1,f_2,\cdots,f_j,\cdots,f_n\}$ 中的每个属性 $f_j\in F$,计算概率 $P(B_f|A_f)$,若 $P(B_f|A_f)>T$,将 f_j 加入 (A,B) 报警相似计算重要属性集。

2) 将满足上述条件的 $P(B_f|A_f)(1\leqslant j\leqslant n)$ 按照降序排序,按照重要性由强到弱的次序进行属性组合,利用上述算法计算组合属性对报警相似的重要性。在计算中舍弃概率值小于 T 的属性组合。

计算中得到的报警类 (A,B) 的最大相关性概率记为 $P(A,B)$,相应的属性组合称为最重要属性组合。

1.3.2 建立报警关联关系并补充攻击图

上述计算的 $P_{(A,B)}$ 是报警类 A 和 B 的条件概率,即当报警 A 出现时,报警 B 已经出现的概率。$P_{(A,B)}>T$ 时,表明 A 与 B 同时出现概率很高;此时 A、B 可能属于同一攻击步骤,或者 B 是 A 的前提攻击步骤。对于满足 $P_{(A,B)}>T$ 的报警对 (A,B),利用前面得到的最重要属性组合计算 A 和 B 的相似度。

设报警对 (A,B) 的最重要属性组合是 $\{f_1,f_2,\cdots,f_n\}$,分析报警 A、B 所对应的攻击行为后为上述属性设定权重系数是 $\{w_1,w_2,\cdots,w_n\}$,例如分析攻击行为后发现两个攻击步骤会利用同一个端口号进行,可为端口属性设定较高的系数。定义向量 $\boldsymbol{X}=\{x_1,x_2,\cdots,x_n\}$,其中若 $(P(B_{fi}|A_{fi})>T$ 或者 $P(A_{fi}|B_{fi})>T)$,$x_i=1$,否则 $x_i=0(i=1,2,\cdots,n)$,两报警相似度值 $S_{(A,B)}=\sum_{i=1}^{n}w_ix_i$。定义报警相似度阈值 S_1 和 S_2 且 $S_1>S_2$,S_1 称为直接相关阈值,S_2 称为间接相关阈值。

利用报警相似度建立报警关联关系。设报警类 $A=\{a_1,a_2,\cdots,a_k\}$ 与攻击图中原子攻击节点不存在映射关系,利用报警相似分析及已知的攻击图将 A 与其他报警类进行关联并补充攻击图的算法如下:

```
1) 初始化队列 Q_C、Q_R 为空;
2) for(每一个已知的报警 X) {
3)   利用(A,X) 的重要属性集计算 P_(A,X) 和 S_(A,X);
4)   if (P_(A,X) ==1) 将(A,X) 插入队列 Q_C 并使 Q_C 按相似度
       S_(A,X) 的非增序排列;
5)   else if (P_(A,X) > T) 将(A,X) 插入队列 Q_R 并使 Q_R 按相似
       度 S_(A,X) 的非增序排列;
6) }
7) while (Q_C 不为空 && (A,B) = 出队(Q_C) && B 与攻击图原
     子攻击没有映射)
8)   if (Q_C 不为空 && S_(A,B) ≥ S_2)
       /* B 与攻击图中原子攻击(设为 e) 有映射关系; */
9)     if (S_(A,B) ≥ S_1)        // 认为 A、B 属于同一攻击步骤;
10)      在A 和 e 之间建立映射关系;在报警图中,将 a_i ∈ {a_1,
           a_2,…,a_k} 与 B 的前提报警中满足属性地址传递关系
           的节点建立关联关系;
11)    else {                    // 认为 B 是 A 的前提攻击步骤;
12)      while(Q_R 不为空 && (A,C) = 出队(Q_R) && C 与
           攻击图原子攻击没有映射);
13)      if(Q_R 不为空 && S_(A,C) > S_2 && C 对应攻击图的原
           子攻击 e_1 是 e 的后果)
           /*A 与 B 的后果步骤 C 属于同一攻击步骤 */
14)        在A 和 e_1 之间建立映射关系;在报警图中,将 a_i ∈
           {a_1,a_2,…,a_k} 与 C 的前提报警中满足属性地
           址传递关系的节点建立关联关系;
15)      else {                  //A 是 B 的后果步骤
16)        在攻击图中新建原子攻击节点 e_1 及后果属性
           节点,将 e 的后果属性节点作为 e_1 的前提属
           性,建立 e_1 与 A 的映射;
17)        在报警图中,将 a_i ∈ {a_1,a_2,…,a_k} 与 B 报警
           中满足属性地址传递关系的节点建立关联
           关系;
18)      }
19)    }
```

20)　else

/ * B 与攻击图中原子攻击没有映射关系或者 $S_{(A,B)} < S_2$ * /;

在攻击图中新建一个孤立的原子攻击节点 e 及其后果属性节点,建立 e 与 A 的映射关系,在报警图中建立报警 $\{a_1,a_2,\cdots,a_k\}$ 及其后果节点;

上述算法对攻击图中没有表示的报警依据报警相似性分析关联报警并对攻击图的缺陷进行补充。

2　实验及结果分析

实现上述混合报警关联模型的原型系统以验证模型的有效性。系统的测评数据选自 MIT Lincoln 实验室开发的 DARPA2000[12] 的 IDS 测评数据集,实验利用了数据集中的攻击场景 LLDOS1. 0;入侵检测系统选用开源 snort(http://www. snort. org),在默认规则下重放上述数据集中的 LLS_DDOS_1. 0-inside. dump 与 LLS_DDOS_1. 0-outside. dump 文件,产生数量为 28 870 条 35 种不同名称的报警。

根据 LLDOS1. 0 的攻击步骤,定义的攻击图如图 3 所示,攻击图中有 7 个原子攻击节点和 6 个属性节点,其中每个原子攻击节点最多有 4 个报警映射,分布式拒绝服务攻击(Distributed Denial of Service,DDoS)相关报警名共有 13 个,所以初始攻击图共有13个报警映射。混合报警关联模型对上述报警数据处理后生成的部分报警图如图 4 所示,报警图清晰地重现了数据集中 DDoS 攻击的入侵过程。

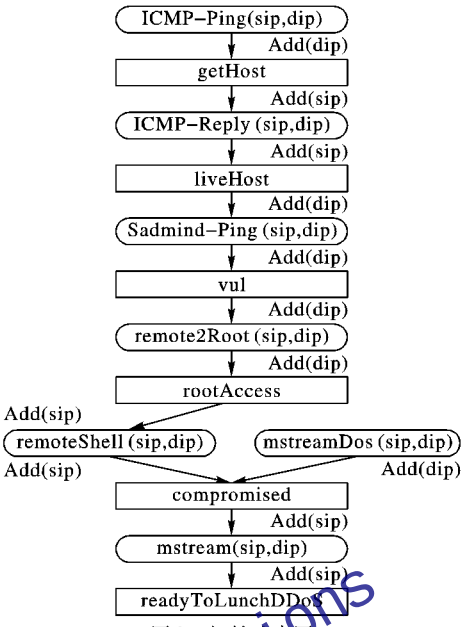

图 3　初始攻击图

图 4　由实验数据得到的报警图片段

混合报警关联模型具有一定的自适应性,利用报警相似性分析可对攻击图的部分定义缺陷进行补充。实验验证了当删除攻击图中的原子攻击节点或攻击节点的报警映射关系时,模型对攻击图缺陷的修复情况如下:

1)若部分删除攻击图中原子攻击与报警的映射关系,且保证每个原子攻击节点至少与一个报警存在映射关系,模型能够完全正确地恢复其他报警映射关系。

2)若攻击图中不存在连续两个原子攻击节点的缺失时,模型能够完全正确地恢复攻击图。

3)若攻击图存在连续多个原子攻击节点的缺失,会造成报警关联的错误,攻击节点的缺失与报警关联错误情况如图 5所示。

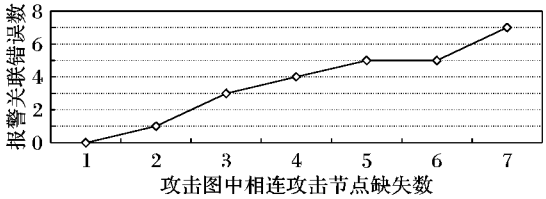

图 5　攻击图中攻击节点缺失与报警关联错误情况

若不定义攻击图,只利用报警的相似性分析进行报警数据关联,报警关联的错误不超过 7 个,因此报警相似性分析使报警关联的正确率有一定的提高。

3 结语

本文提出了一种基于攻击图与报警数据相似性分析的混合报警关联模型。模型首先在报警数据预处理中消除了 IDS 产生的周期性误报警和重复报警，然后将预处理后的报警数据根据攻击图或报警相似度进行关联，进而重构入侵攻击场景。模型能够对初始攻击图的定义缺陷利用报警数据相似分析进行完善与补充。实验验证了混合模型的有效性。

模型中报警相似度计算的属性权值和判断阈值是人工设定的，权值的设定与具体的攻击类型相关，因此限制模型的应用范围。进一步的工作将利用学习的方法调整报警相似性分析的判断阈值，使其能够适应网络环境和攻击的变化。

参考文献：

[1] MAINES J, KEWLEY D, TINNEL L, *et al*. Validation of sensor alert correlators [J]. IEEE Security & Privacy Magazine, 2003, 1(1): 46 – 56.

[2] NING P, YUN C, REEVES D S, *et al*. Techniques and tools for analyzing intrusion alerts[J]. ACM Transactions on Information and System Security, 2004, 7(2): 274 – 318.

[3] DEBAR H, WESPI A. Aggregation and correlation of intrusion-detection alerts [C]// RAID 2001: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, LNCS 2212. Berlin: Springer-Verlag, 2001: 85 – 103.

[4] VALDES A, SKINNER K. Probabilistic alert correlation [C]// RAID 2001: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, LNCS 2212. Berlin: Springer-Verlag, 2001: 54 – 68.

[5] REN H, STAKHANOVA N. An online adaptive approach to alert correlation [C]// DIMVA 2010: Proceedings of the 7th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer-Verlag, 2010: 153 – 172.

[6] AHMADINEJAD S H. A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs[J]. Computer Networks, 2011, 55(9): 2221 – 2240.

[7] AHMADINEJAD S H, JALILI S. Alert correlation using correlation probability estimation and time windows [C]// ICCTD 2009: Proceedings of the 2009 International Conference on Computer Technology and Development. Piscataway, NJ: IEEE Press, 2009: 170 – 175.

[8] CURRY D, DEBAR H. Intrusion detection message exchange format data model and extensible markup language (XML) document type definition [EB/OL]. [2007-05-01]. http://tools.ietf.org/html/rfc4765.2003.

[9] LI D, LI Z, LEI J. Research on the method of reducing false positives with periodicity[J]. Journal of Chinese Computer Systems, 2009, 30(7): 2446 – 2449. (李东, 李之棠, 雷杰. 周期性误告警去除方法研究[J]. 小型微型计算机系统, 2009, 30(7): 1336 – 1340.)

[10] GUO F, YU M, YE J. Alert aggregation algorithm based on category and similarity[J]. Journal of Computer Applications, 2007, 27(10): 2446 – 2449. (郭帆, 余敏, 叶继华. 一种基于分类和相似度的报警聚合方法[J]. 计算机应用, 2007, 27(10): 2446 – 2449.)

[11] CHEN F, ZHANG Y, SU J, *et al*. Two formal analyses of attack graphs[J]. Journal of Software, 2010, 21(4): 838 – 848. (陈锋, 张怡, 苏金树. 攻击图的两种形式化分析[J]. 软件学报, 2010, 21(4): 838 – 848.)

[12] MIT/LL. 2000 DARPA intrusion detection scenario specific datasets[EB/OL]. [2010-03-26]. http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_index.html.

(上接第 72 页)

4 结语

综合 Biclique 攻击在分组密码安全性分析中的现有应用，可以发现 Biclique 攻击适合应用于密钥扩展策略简单、扩散层混淆速度较慢的算法，而与非线性 S 盒的具体设计无关。考虑这两种因素，本文选择建立 ARIRANG-256 的 0 到第 8 轮 32 维 Biclique，对完整 40 轮的 ARIRANG-256 应用 Biclique 攻击，得到了优于穷举攻击的计算复杂度。与 ARIRANG-256 已有的分析结果相比，本文分析结果的优势体现为全轮攻击且数据复杂度足够小，是 Biclique 攻击在分组密码全轮安全性分析中的又一次成功应用。考虑到 Biclique 攻击较大的计算复杂度，以后的研究方向为 Biclique 攻击在分组密码中应用的改进，进一步减少其计算复杂度。

参考文献：

[1] CHANG D, HONG S, KANG G. ARIRANG: SHA-3 proposal[EB/OL]. [2009-10-10]. http://csrc.nist.govgroups/ST/hash/sha-3/Round1/documents/ARIRANG.zip.

[2] GUO J, MATUSIEWICZ K, KNUDSEN L R. Practical pseudo-collisions for Hash functions ARIRANG-224/384[M]. Berlin: Springer-Verlag, 2009: 141 – 156.

[3] HONG D, KOO B, KIM W H. Preimage attacks on reduced steps of ARIRANG and PKC 98-hash[C]// Proceedings of ICISC 2009. Seoul: [s.n.], 2009: 315 – 331.

[4] ZHANG P, LI R L, LI C. Related-key rectangle attack on the full ARIRANG encryption mode[J]. Journal on Communications, 2011, 32(8): 15 – 22. (张鹏, 李瑞林, 李超. 对完整轮数 ARIRANG 加密模式的相关密钥矩形攻击[J]. 通信学报, 2011, 32(8): 15 – 22.)

[5] KHOVRATOVICH D, RECHBERGER C, SAVELIEVA A. Bicliques for preimages: attacks on Skein-512 and the SHA-2 family [EB. OL]. [2012-10-10]. http://eprint.iacr.org/2011/286.

[6] BOGDANOV A, KHOVRATOVICH D, RECHBERGER C. Biclique cryptanalysis of the full AES[C]// Proceedings of ASIACRYPT 2011, LNCS 7073. Berlin: Springer-Verlag, 2011: 344 – 371.

[7] MALA H. Biclique cryptanalysis of the block cipher SQUARE[EB/OL]. [2012-10-10]. http://eprint.iacr.org/2011/500.

[8] HONG D, KOO B, KWON D. Biclique attack on the full HIGHT [C]// Proceedings of ICISC 2011, LNCS 7259. Berlin: Springer-Verlag, 2011: 365 – 374.

[9] CHEN S, XU T. Biclique attack of the full ARIA-256[EB/OL]. [2013-02-01]. http://eprint.iacr.org/2012/011.pdf.

[10] COBAN M, KARAKOC F, BOZTAS O. Biclique cryptanalysis of TWINE[EB/OL]. [2013-02-01]. http://eprint.iacr.org/2012/422.pdf.

[11] WANG Y, WU W, YU X. Biclique cryptanalysis of reduced-round piccolo block cipher[C]// Proceedings of ISPEC 2012, LNCS 7232. Berlin: Springer-Verlag, 2012: 337 – 352.

[12] ABED F, FORLER C, LIST E, *et al*. Biclique cryptanalysis of the PRESENT and LED lightweight ciphers[EB/OL]. [2013-02-01]. http://eprint.iacr.org/2012/591.pdf.