Computer Science and Application 计算机科学与应用, 2020, 10(12), 2431-2438
Published Online December 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.1012258

Hans汉斯

基于机器学习的网络安全态势感知

杨　怡[1*]，边　媛[2]，张天桥[1]

[1]32021部队，北京
[2]空军工程大学装备管理与无人机工程学院教学科研处，陕西　西安
Email: *972087842@qq.com

收稿日期：2020年11月29日；录用日期：2020年12月24日；发布日期：2020年12月31日

摘　要

在传统网络防御手段抵御攻击的基础上，提出了一种利用机器学习的方法来达到网络安全态势感知的新方案。为了有效地获得告警事件，本文引入了告警关联分析的技术，通过分析多源告警信息的关联度从而降低误报率；为了准确地重建攻击场景，本文引入CEP技术处理海量告警信息，并利用基于马尔可夫性质的因果关联分析构建起知识库。分析表明，该方案具有可靠性强、适用性好、计算量小、准确度高的特点，特别适合于大数据环境。

关键词

机器学习，态势感知，关联分析，攻击场景重建

The Network Security Situation Awareness Based on Machine Learning

Yi Yang[1], Yuan Bian[2], Tianqiao Zhang[1]

[1]32021 Troop, Beijing
[2]Air Force Engineering University, Xi'an Shaanxi
Email: *972087842@qq.com

Received: Nov. 29th, 2020; accepted: Dec. 24th, 2020; published: Dec. 31st, 2020

Abstract

On the basis of the traditional network defense means to resist the attack, a new scheme using machine learning method to achieve network security situational awareness is proposed. In order to obtain alarm events effectively, this paper introduces the technology of alarm correlation anal-

*通讯作者。

文章引用: 杨怡, 边媛, 张天桥. 基于机器学习的网络安全态势感知[J]. 计算机科学与应用, 2020, 10(12): 2431-2438.
DOI: 10.12677/csa.2020.1012258

ysis, which reduces the false alarm rate by analyzing the correlation degree of multi-source alarm information. In order to reconstruct the attack scene accurately, this paper introduces the CEP technology to deal with the massive alarm information, and uses the causal association analysis based on Markov property to build the knowledge base. The analysis shows that the scheme has the characteristics of strong reliability, good applicability, small calculation amount and high accuracy, and is especially suitable for big data environment.

Keywords

Machine Learning, Network Situation Awareness, Association Analysis, Attack Scene Reconstruction

1. 引言

随着信息技术的飞跃式发展和互联网的快速普及，用户在体验到新技术带来的便捷、高效的同时也深受网络攻击引发的破坏。目前，我们熟知的网络威胁有：网络病毒、木马、DOS/DDOS 攻击等等。这些攻击带来的告警信息是海量的，冗余的，然而传统的网络安全技术还不能完全地、及时地处理这些告警数据。

现今主流的网络防御手段还是在保护、检测、响应的模型下开展的。虽然一个网络环境中部署多个安全防御设备起到了一定的作用，但是却在工作的同时产生了大量的，价值密度低的告警和日志信息。通常情况下一个攻击往往是分多步实施的，但告警信息却只指针对于其中某一步，是单一的，分散的，以至于还原攻击场景或是攻击过程是困难的。因此这些大量的、繁杂的安全事件数据不仅没有有效地对攻击进行防御，还在无形中给决策者带来了更大的工作量。网络安全态势感知就是将网络攻击场景通过重建的方式，有效地，准确地还原攻击活动的全貌，达到对整个网络安全态势进行监控的目的，这在网络安全防御中显得至关重要，这也是网络安全态势感知领域中面临的一个难题之一。

针对网络攻击高效的告警预测提出一种基于机器学习的网络安全态势感知的关联分析方法[1]，利用该方法获取价值密度高的告警事件，通过聚类、关联分析构建出规则知识库，并对攻击场景进行重建，从而达到告警预测的目的。

2. 基于地址相关性的告警事件聚类

利用因果关联分析的方法进行关联分析，首先是要把具有相关性的告警事件聚成一类，然后对同一类簇中的告警事件进行因果关联分析[2]。具体而言聚类就是把抽象的对象集合根据类似的特征分成多个类的过程。首先把原始告警数据进行预处理，对来自不同安全设备的告警事件进行统一格式，提取出不同事件关键的描述字段，包括以下 12 条属性，用这 12 条属性就可以清楚的描述一个安全事件。如表 1 所示。

根据告警事件处理的原则，依照事件严重等级、攻击行为强度、攻击持续时间等依据从 12 条属性中挑选出具有代表性的 7 个属性作为告警事件聚类时的匹配格式：

$a_i = (\text{attacktime}, \text{attacktype}, \text{sourceIP}, \text{sourcePort}, \text{targetIP}, \text{targetPort}, \text{severity})$ 其中 attacktime 是安全事件发生的时间；attacktype 是安全事件所属的类型；sourceIP 是发起攻击或安全事件中的源 IP 地址；sourcePort 是发起安全事件发生的源端口；targetIP 是发起攻击或安全事件中的目的 IP 地址；targetPort 是发起安全事件发生的目标端口；severity 是安全事件所属的威胁等级。

Table 1. Key fields of a security event
表 1. 安全事件的关键字段

关键字段	关键字段
DeviceID	发生安全事件所属的设备名称或设备编号
AttackDate	安全事件发生的日期
AttackTime	安全事件发生的时间
AttackType	安全事件所属的类型
SourceIP	发起攻击或安全事件中的源 IP 地址
TargetIP	发起攻击或安全事件中的目的 IP 地址
SourceName	安全事件中源设备名称
TargetName	安全事件中目标主机名称
SourcePort	发起安全事件发生的源端口
TargetPort	发起安全事件发生的目标端口
Severity	安全事件所属的威胁等级
Occurrence	安全事件发生的次数

由于例如一个 DDOS 攻击，它们攻击的每一步之间的 IP 地址一定存在相关性，所以就可以利用 IP 相关性进行聚类。同样地，其他的攻击也一定存在着这种相关性。那么就可以根据多步攻击之间的 IP 地址肯定具有相关性，即上一步的攻击 a_1 中目的 IP 很有可能是下一个攻击 a_2 的源 IP，或者说上一个攻击 a_1 的源 IP 地址或目的 IP 地址之中总有一个和攻击 a_2 的目的地址或源地址相同。快速把告警事件聚类在一起。如图 1 是聚类的流程图。

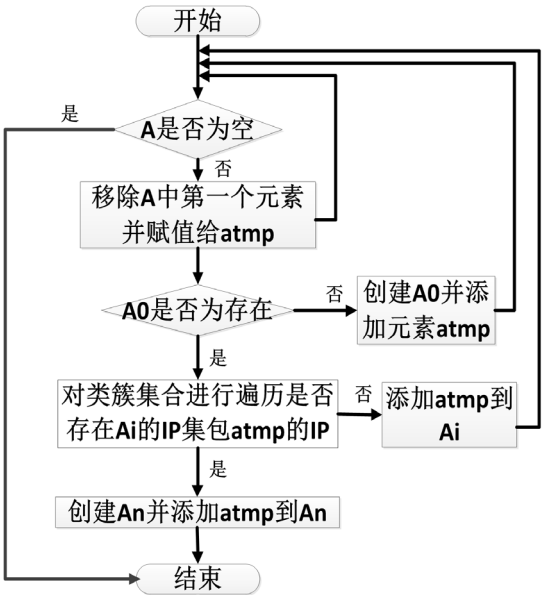

Figure 1. Flow chart based on alarm clustering algorithm
图 1. 基于告警聚类算法的流程图

3. 攻击场景重建

将分散的告警事件依据地址相关性进行聚类后，得到了一个个的告警类簇。下面就是要根据这些类

簇展开关联分析。具体地：通过统计大量告警事件，分析上一个告警事件发生后到下一个告警事件发生它们之间的必然联系，即上一个事件发生后下一个事件一定发生的可能性大小，然后根据实际需求人为的设置好的支持度 a，当支持度达到值 a 的时候，就认为它们两个攻击之间的发生存在必然性，就可以将它们之间的关联度纳入规则知识库中，这样就在关联分析的同时建立了关联规则知识库，有利于在发现新的告警的时候实时地增加进去[3]。

如图 2 所示，是对假设可能的攻击行为构建的一步转移概率矩阵模型，将告警事件写成行列的形式，表示各个告警事件发生之间的关联度。例如 0.4 表示当告警事件 a 发生后 b 发生的概率为 0.4。在一步转移概率矩阵 $D=\{d_{ij}\}$ 中每一个元素 d_{ij} 表示当前时刻 i 到下一时刻 j 的条件概率为 $p(i|j)$。因为马尔可夫链的性质要求各个状态的转移概率之和必须为 1，这样就得到了一个个独立的因果知识矩阵。假如当遍历一个告警序列时，出现了新的告警事件类型，这时只要在矩阵中再加入新的一行 $(ai+1)$ 一列 $(aj+1)$，这样既能确保矩阵完全包含新的攻击类型，又能快速加入新出现的告警类型，做到实时检测，动态添加，不重不漏。

Attack Types	a	b	c	d	e	f	g
a	0	0.4	0.6	0	0	0	0
b	0	0	0.7	0.3	0	0	0
c	0	0	0	1.0	0	0	0
d	0	0	0	0	0.5	0.1	0.4
e	0	0	0	0	0.7	0.3	0
f	0	0	0	0.8	0	0.2	0
g	0	0	0	0	0	0.4	0.6

Figure 2. A one-step transition probability matrix between attack types
图 2. 攻击类型间的一步转移概率矩阵

图 2 也可以用马尔可夫链模型来表示，其中的每一个状态都代表一个攻击类型，各个状态之间的转移概率表示一个攻击转移到下一个攻击的条件概率。因为马尔可夫链具有无后效性，也就是说，每一个攻击的发生只与它的上一个攻击有关，与其它均无关。如图 3 所示，即

$$p(x_{i+1}|x_i, x_{i-1}, \cdots, x_1) = p(x_{i+1}|x_i)。$$

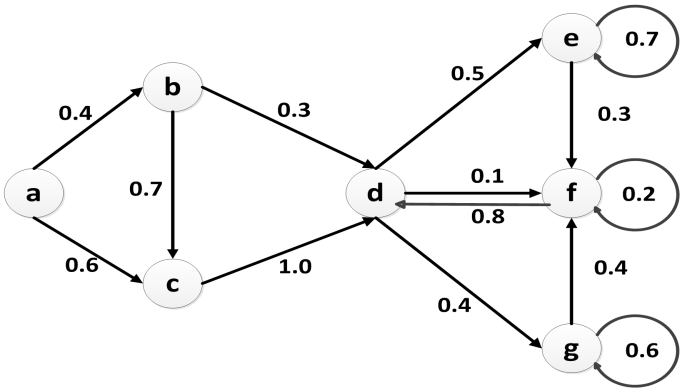

Figure 3. Markov chain model
图 3. 马尔可夫链模型

4. 系统测试

4.1. 整体方案设计

为了实现网络安全态势的动态感知和实时的告警预测，需要对告警事件进行深入挖掘，研究告警事件之间存在的某些必然联系，进而利用它们的关联关系，分析并掌握整个网络的发展趋势，从而达到态势感知的目的[4]。为此设计了如图 4 的方案整体框架：

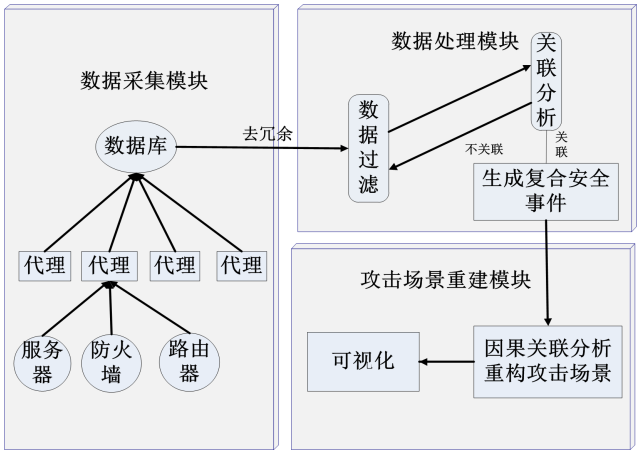

Figure 4. Overall scheme framework
图 4. 方案整体框架

利用三个模块构建对告警数据进行采集、预处理、关联分析最终到攻击场景重建。

数据采集模块：利用搭建的数据处理平台中的各个代理从不同环境采集系统日志信息、应用日志信息、安全日志信息和网络日志信息等格式未统一的数据，然后经过数据库统一整合后将这些信息递交给数据处理模块。

数据处理模块：由于从数据采集模块获得的安全事件格式是不一致的，而且它们往往存在重复冗余、误报率高、分散独立、价值密度低等问题。利用数据处理模块中已有的告警数据库比对，首先对这些数据进行预处理，合并在同一时刻重复的信息，去除误报信息，将针对同一属性的信息进行聚类融合，并统一格式，这个过程同时是迭代更新的，不断比对告警数据，不断增加新的告警信息[5]。针对每一个告警类簇进行关联分析，统计出每条攻击之间的关联度，并构建起规则知识库。

攻击场景重建模块：再根据得到的具有关联规则的安全事件，还原出攻击场景，并提交到控制中心，当接下来再得到安全事件时，可直接与规则知识库进行匹配，来判断攻击类型。供决策者进行下一步处理。

4.2. 方案实现

测试采用的是 DARPA2000 的攻击场景测评数据集 LLDOS1.0 来进行因果关联分析的。DARPA2000 是当下最具权威性的入侵检测攻击场景测评数据集，并被广泛用于验证针对各类告警事件的关联规则的有效性中。

DARPA2000 是一个 DDOS 攻击的测评数据集，具体的攻击过程可以分为五个阶段，如图 5 所示：预探测网络环境，也就是初步探测是否具备攻击条件，漏洞扫描，通过扫描获得多个可以实施攻击的漏洞，root 权限获取，安装木马软件以及实施远程 DDOS 攻击。

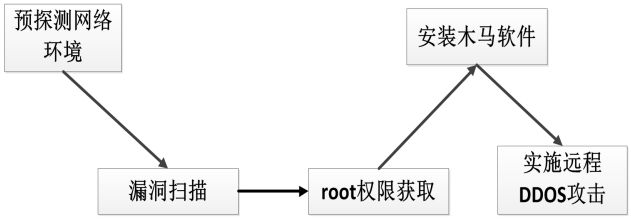

Figure 5. DDOS Attack process based on sadmind vulnerability
图 5. 根据 Sadmind 漏洞进行的 DDOS 攻击流程

首先针对这五个阶段的告警事件进行基于地址相关性的聚类，从而得到了 6 个类簇：$A_1 \sim A_6$ 然后再利用基于马尔可夫性质的因果关联知识挖掘算法对得到的 6 个告警类簇进行因果知识挖掘。得到同一类簇中各告警之间的关联度，如表 2 所示[6]。

Table 2. The attack step is related to the corresponding alarm
表 2. 攻击步骤对对应的告警关联度

上一个攻击告警	下一个攻击告警	关联度
ICMP PING	RPC Sadmind UDP PING	0.315
RPC Sadmind UDP PING	RPC sadmind query with root credentials attempt UDP	0.719
RPC sadmind UDP NETMGT_PROC_SERVICE CLIENT_DOMAIN overflow attempt	RSERVICES rsh root	0.240
RSERVICES rsh root	DDOS mstream Handler to client	0.643
DDOS mstream Handler to client	SNMP request udp	0.547
RPC sadmind query with root credentials attempt UDP	RPC sadmind UDP NETMGT_PROC_SERVICE CLIENT_DOMAIN overflow attempt	0.584
SNMP request udp	BAD-TRAFFIC Loopback traffic	0.351

然后对各个攻击类型进行编号，如表 3 所示：

Table 3. Attack types and their corresponding Numbers
表 3. 攻击类型及其对应编号

节点序号	攻击类型
1	ICMP PING
2	FTP Bad Login
3	TELNET Bad Login
4	RPC Sadmind UDP PING
5	RPC sadmind query with root credentials attempt UDP
6	RPC sadmind UDP NETMGT_PROC_SERVICE CLIENT_DOMAIN overflow attempt
7	WEB-IIS%2E-asp access
8	RSERVICES rsh root
9	DDOS mstream Handler to client
10	DDOS mstream client to Handler
11	SNMP request udp
12	BAD-TRAFFIC Loopback traffic

根据因果知识关联分析算法所得到的攻击类型之间的转移概率，再结合表 2 对各攻击类型的编号可以得出 12 种攻击类型的 12 * 12 转移概率矩阵[7]。矩阵中各行和各列所对应的数值表示发生该行告警事件后发生该列告警事件的概率。例如 a_{12} = 0.633 表示当发生告警事件 1 (ICMP PING)后发生告警事件 2 (FTP Bad Login)和转移概率为 0.633。如图 6 所示：

0.633	0.025	0.127	0.315	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
0.439	0.561	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
0.000	0.000	0.769	0.231	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
0.000	0.000	0.000	0.624	0.719	0.257	0.000	0.000	0.000	0.000	0.000	0.000
0.000	0.000	0.000	0.000	0.443	0.584	0.000	0.000	0.000	0.000	0.000	0.000
0.000	0.000	0.000	0.201	0.000	0.397	0.142	0.240	0.000	0.000	0.000	0.000
0.000	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.250	0.643	0.250	0.000	0.000
0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.667	0.547	0.000
0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000
0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.857	0.351
0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000

Figure 6. Based on DARPA2000 alarm type shift probability matrix
图 6. 基于 DARPA2000 告警攻击类型转移概率矩阵

图 7 是对概率矩阵图形化的表示，也是一个完整的攻击场景重建。

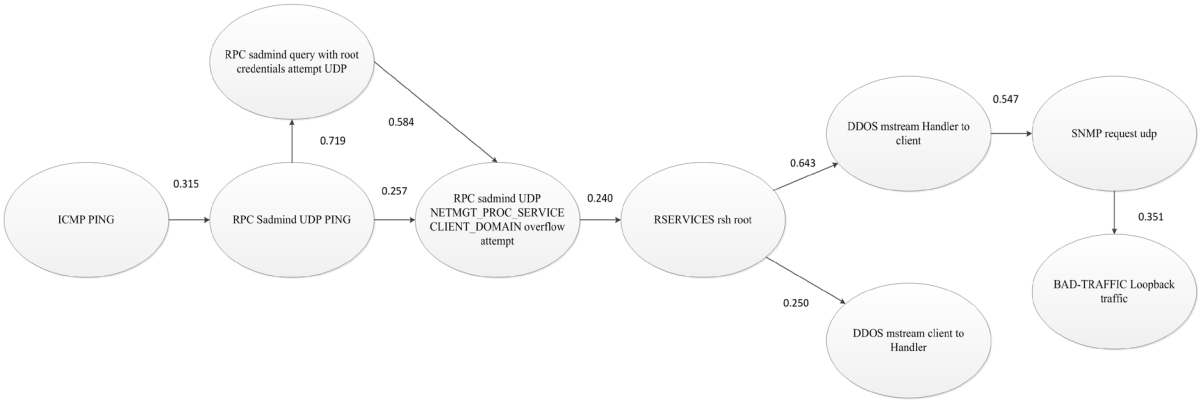

Figure 7. Causal knowledge of markov chain models for DDOS attack scenarios
图 7. DDOS 攻击场景的马尔可夫链模型因果知识

根据攻击场景的重现，可以直观地展示出 DDOS 攻击的全过程，它主要分为了五个阶段：预探测网络环境(RPC Sadmind UDP PING)、漏洞的扫描(RPC sadmind UDP NETMGT_PROC_SERVICE CLIENT_DOMAIN overflow attempt)、利用 solaris 的漏洞 sadmind 进入系统(RSERVICES rsh root)、安装木马软件 mstream DDOS (DDOS mstream Handler to client 或 DDOS mstream client to Handler)以及发起远程 DDOS 攻击(BAD-TRAFFIC Loopback traffic)。并且清楚地看到每一步攻击之间的转移概率为：a_{46} = 0.257、a_{68} = 0.260、a_{89} = 0.500 或 a_{810} = 0.250 以及 $a_{11,12}$ = 0.143。也可以发现，攻击者在采取关键攻击的同时，也会尝试采取一些其他的攻击活动。

5. 结束语

本课题主要研究了基于机器学习的网络安全态势感知技术，以机器学习方法作为主要手段，将关联分析法和事件因果关系相结合，在构建贝叶斯网络的基础下，对数据进行去除、分类和识别等处理，然后利用马尔可夫链模型，产生概率矩阵并构建出动态规则知识库。从而达到告警预测和攻击场景重

建的目的，并向决策者提供处理意见。对传统的网络安全监控进行了改进，更适用于大数据、复杂网络的环境下。

通过试验发现各个看似独立分散的告警数据之间的确存在着必然的联系，例如源 IP 或目的 IP 地址相同的告警事件就很有可能是一个攻击行为中多个步骤。利用机器学习中因果关联分析的方法在对数据从采集、挖掘、处理到分析的全过程中，可以有效地快速地挖掘告警数据之间的关联度，并建立起规则知识库，从而达到针对现有的告警事件推测出下一步具有大概率发生的攻击的可能性，也能够对已发生的攻击进行场景还原，得到可视化的转移图，更加直观地为决策者提供支持。测试结果表明：

1) 一个攻击行为的确是分为多步实施的；
2) 具有地址相关性的告警事件的确存在必然联系；
3) 针对告警事件关联度预测可能发生的攻击是有效，可靠的；
4) 基于马尔可夫性质的告警关联规则能够更好地满足攻击种类不断更新的现状；
5) 因果知识库的动态建立提高了效率，更加适应于大数据环境下；
6) 对攻击类型一步转移矩阵的图形化表示，更加直观，清晰，有利于对网络态势的整体掌握。

基金项目

本文受国家高新技术研究发展计划(863)项目(2008AA01Z404)资助。

参考文献

[1] 王莉. 网络多步攻击识别方法研究[D]: [博士学位论文]. 武汉: 华中科技大学, 2007.
[2] 刘必雄. 多源异构日志综合分析技术研究与实践[J]. 南京信息工程大学学报, 2011, 3(4): 365-370.
[3] 冯学伟, 王东霞, 黄敏桓, 等. 一种基于马尔可夫性质的因果知识挖掘方法[J]. 计算机研究与发展, 2014, 51(11): 2493-2504.
[4] 马东君. 网络安全态势感知技术与系统[J]. 网络安全技术与应用, 2013(11): 70-71.
[5] 胡卫华, 张利, 刘锡峰. 安全事件采集关键技术研究与实现[J]. 计算机应用与软件, 2012, 29(12): 309-314
[6] 王文槿, 刘宝旭. 一种基于关联规则挖掘的入侵检测系统[J]. 核电子学与探测技术, 2015(2): 119-123.
[7] 冯学伟. 一种基于概率转移的 Cyber 攻击场景感知推理技术[J]. 指挥与控制学报, 2015(1): 62-67.