doi:10.11887/j.cn.201705021　　http://journal.nudt.edu.cn

运用警报关联的威胁行为检测技术综述*

王意洁[1],程　力[1],马行空[2]
(1. 国防科技大学 计算机学院 并行与分布处理重点实验室,湖南 长沙　410073;
2. 国防科技大学 计算机学院 网络工程系,湖南 长沙　410073)

摘　要:基于警报关联的网络威胁行为检测技术因其与网络上大量部署的安全产品耦合,且能充分挖掘异常事件之间的关联关系以提供场景还原证据,正成为复杂威胁行为检测的研究热点。从威胁行为和网络安全环境的特点出发,引出威胁行为检测的应用需求和分类,介绍基于警报关联的威胁行为检测的基本概念和系统模型;重点论述作为模型核心的警报关联方法,并分类介绍了各类典型算法的基本原理和特点,包括基于因果逻辑的方法、基于场景的方法、基于相似性的方法和基于数据挖掘的方法;并结合实例介绍了威胁行为检测系统的三种典型结构,即集中式结构、层次式结构和分布式结构;基于当前研究现状,提出了对未来研究趋势的一些认识。

关键词:威胁行为检测;警报关联;检测模型;检测系统结构
中图分类号:TP393　　**文献标志码**:A　　**文章编号**:1001-2486(2017)05-128-11

Survey of alert-correlation based on network threat detection techniques

WANG Yijie[1], *CHENG Li*[1], *MA Xingkong*[2]
(1. National Key Laboratory for Parallel and Distributed Processing, College of Computer, National University of Defense Technology, Changsha 410073, China;
2. Department of Network Engineering, College of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract: The rapid development of the Internet also causes more and more network threats. How to detect the network threats in a real-time and accurate manner becomes one of the key technique issues. The alert-correlation-based network threat detection technique is becoming the research hotspot, which couples with the widely used security products and fully exploits the relation between abnormal events to reconstruct the attack scenario. Starting from the features of network threats and security environment, the requirements and classification of network threat detection were introduced. Then the basic concepts and system model of alert-correlation-based network threat detection technique were illustrated in detail. The key module of the model, alert correlation method, and the fundamentals and features of different kinds of typical algorithm were studied in detail, including causal-relation-based method, case-based method, similarity-based method and data-mining-based method. Furthermore, three kinds of representative detection system architectures were discussed with practical instances, namely centralized architecture, hierarchical architecture and distributed architecture. Finally, based on the analysis of recent research work, the future work is discussed and outlined.

Key words: network threat detection; alert correlation; detection model; detection system architecture

互联网的不断发展使其面临着越来越多的网络安全威胁,目前典型威胁行为有僵尸网络攻击(Botnet)、分布式拒绝服务攻击(Distributed Denial of Service, DDoS)、蠕虫攻击(Worm)和FTP Bounce Attack 等[1]。这些恶意威胁行为,使网络安全领域面临严峻的考验与挑战,并直接或间接地威胁到了国家安全。因此,如何实时准确地检测网络威胁行为是当前亟须解决的关键问题。

基于警报关联的网络威胁行为检测技术因其与网络上大量部署的安全产品耦合,且能充分挖掘异常事件之间的关联关系以提供场景还原证据,正成为威胁行为检测的研究热点,众多的国内外知名会议和期刊中涌现出了大批的研究成果。本文介绍了各种典型的基于警报关联

* **收稿日期**:2016-05-11
基金项目:国家自然科学基金资助项目(61379052);国家 863 计划资助项目(2013AA01A213);湖南省自然科学基金杰出青年基金资助项目(14JJ1026);高等学校博士学科点专项科研基金资助课题(20124307110015)
作者简介:王意洁(1971—),女,北京人,教授,博士,博士生导师,Email: wangyijie@nudt.edu.cn

的威胁行为检测方法,试图较为全面地综述近年来的最新研究成果,期望对此领域的研究者们有所帮助。

1　威胁行为检测

1.1　威胁行为特点

网络威胁行为种类繁多,且出现频率越来越高,往往具有以下特点:

1)多步行为,即一次网络威胁行为往往包括多个步骤。例如一个针对 Windows 平台 ms08 - 067 漏洞的缓冲区溢出攻击,攻击者经过网络扫描、漏洞探测、网络渗透和安装木马等多个步骤来完成整个攻击[2]。

2)时间跨度长,即属于同一威胁行为的多个步骤可能间隔时间较长。例如僵尸网络在感染大量主机后,有可能会长时间地潜伏,在需要时控制被感染主机以达到恶意目的[3]。

3)变异性强,即威胁行为的手段随着时间的推移不断升级。安全厂商推出安全产品进行防御,而攻击者会更新代码推出升级版的攻击手段,以绕开防御措施的检测[4]。

1.2　威胁行为检测应用需求

信息技术的发展使得网络规模不断增大,同时也使得网络环境安全形势更加严峻,存在一些较为突出的特点,主要表现在:

1)数据规模大:一方面,网络规模的扩大和高速网络技术的发展必然会产生大规模的数据;另一方面,威胁行为的不断增多也会增加数据生成量。

2)网络数据冗余:网络数据中包含大量有正常网络活动引起的与威胁行为无关的冗余数据[4]。

3)威胁行为多样性:发起者会更新已有方法或采用新的技术手段,导致威胁行为不仅包含已知行为类型,还包含有大量未知的类型[5]。

根据网络环境的以上特点,为消除或最大限度地降低网络威胁行为带来的损失,威胁行为检测技术需要同时满足如下需求:

实时性:即系统有能力快速处理数据,适应高速数据流。

准确性:即系统有能力从大量数据中准确发现异常,还原威胁行为。

自适应性:即能够根据网络行为的变化进行调整,有效检测未知威胁行为类型。

在以上需求中,准确性是评判威胁检测技术最根本的标准,实时性则是要求在第一时间发现威胁行为以避免更大程度的损失,自适应性是任何威胁检测技术都追求的目标。如何满足这些需求成为各类威胁检测技术所面临的关键问题。

1.3　威胁行为检测分类

根据分析数据源的不同,威胁行为检测技术可分为基于流量分析的威胁行为检测方法、基于网络数据包分析的威胁行为检测方法和基于警报关联的威胁行为检测方法[1]。

基于流量分析的威胁行为检测方法的分析源数据为网络的流量数据,其基本思想是将网络上的流量变化与正常(异常)情况下的流量变化进行对比分析,判断是否发生威胁行为,这种方法数据形式简单,数据量较小,但只能针对会引起明显流量异常的威胁行为类型;基于网络数据包分析的威胁行为检测方法则是通过解析网络数据包检测威胁行为,这种方法使用的数据包含信息量最大,理论上检测威胁行为精度最高,但是数据量过于庞大,且形式较为复杂,实施难度较大;基于警报关联的威胁行为检测方法则是上述两种的折中,其分析源数据来自安全产品产生的警报数据,网络数据包经过滤后数据量减小,且产生的警报数据包含其中关键信息,该方法检测能力较强,但需要解决外界环境和安全产品带来的若干问题。

由于威胁行为的判断涉及较强的专业领域性,威胁行为检测方法往往需要先验知识和专家知识。根据是否需要先验知识,可分为两类。需要先验知识的典型方法包括基于因果逻辑的方法、基于场景的方法,这类方法基于专家规则对数据进行对比分析;不需要先验知识的典型方法包括基于相似性的方法、基于数据挖掘的方法,这类方法通过主动挖掘数据中关联关系进行威胁行为检测。根据检测威胁行为范围,威胁行为检测可分为特定类型威胁行为检测方法、已知威胁行为检测方法和未知威胁行为检测方法。特定类型威胁行为检测方法根据指定行为特点建立针对性检测模型,已知威胁行为检测方法和未知威胁行为检测方法根据是否具有未知类型检测能力来区别[5]。

2　基于警报关联的威胁行为检测概述

为了检测网络上的异常事件,互联网上大量部署以入侵检测系统(Intrusion Detection System, IDS)为代表的安全产品。通过在互联网上的若干关键节点部署安全产品,收集网络数据并进行分析,依据预先定义的安全策略判定是否为网络

异常事件[4]。部署在互联网上的安全产品会产生大量的警报,这些数据能成为网络威胁行为检测、防御和响应的重要依据。

对于网络威胁行为,一次完整的行为往往包含多个步骤,也就对应着多个异常事件警报,单独地分析这些警报代表的单一安全事件是难以得到更为全面的信息。因此,需要基于警报关联的复杂威胁行为检测方法对生成的警报数据进行综合分析处理,将疑似属于同一威胁行为的多个警报关联起来,甄别其中具有价值的异常事件,揭示出隐藏的关联关系,还原威胁行为场景,从而及时做出响应,有效控制网络安全态势[1]。

2.1 警报数据特点

警报数据由网络安全环境和安全产品共同产生。网络基础设施规模巨大,且环境动态变化,导致产生的警报数据具有以下特点:①警报数据流高速到达且警报类型分布往往是偏斜的,以深圳某骨干网上收集到的数据为例,每天收集到的 Snort 警报数据量约 900 万条,其中出现频率最高的前 20% 的警报占该数据量的 80% 以上[5];②网络警报数据类型分布动态变化,网络环境的变化促使网络威胁行为的更新与升级,导致新警报数据的不断产生,从而引起了数据类型分布的不断变化。

由于安全产品目前尚存在许多问题,导致产生的警报数据具有以下特点[4,6]:①数据冗余量大,安全产品的规则之间存在较大的交集,导致同一异常事件所引发的警报常常不止一条,从而使得安全数据包含较多重复信息和冗余数据;②误报问题严重,一方面,为防止漏报,安全厂商往往提高安全产品的阀值,导致很多正常的网络活动会被识别为异常事件,引发警报;另一方面,网络环境的变化会引起网络活动性质的变化,而安全产品的更新速度往往落后于环境变化,因此也会产生一些错误数据;③安全数据相对分散、独立,难以建立联系,安全产品通常只根据事先定义的异常事件特征库,对网络数据进行简单的模式匹配,只能检测出孤立的异常网络事件[7]。因此,需要警报关联技术对这些警报数据进行进一步全面关联分析,过滤其中的冗余信息,提取有价值的信息,对各类威胁行为进行有效检测。

2.2 技术挑战

大规模网络环境下,多样化威胁行为高频率出现,产生大量分布动态变化的警报数据。为了满足实时性、准确性和自适应性的要求,基于警报关联的威胁行为检测技术面临以下四个方面的技术挑战。

1)海量警报数据引起的检测效率问题。大规模网络环境下网络威胁行为的高频率出现,使得短时间内会有大量的警报数据产生,要求系统具备高匹配吞吐率。同时,网络活动的变化使得这些警报数据的类型分布也在动态变化,要求系统具备相应的调整机制。因此,如何针对海量分布动态变化警报数据设计实时威胁行为检测算法是当前基于警报关联的威胁行为检测技术研究中的关键问题。

2)长时间跨度威胁引起的检测开销问题。部分复杂威胁行为时间跨度较长,算法需要处理长时间累积的大量警报数据,要求系统能够降低开销。资源开销直接决定系统能够同时处理的警报数目。低资源开销能够支持更长的监测窗口,同时进行关联的警报数目更多,从而得到更完备的结果。因此,如何针对海量警报数据设计低开销的威胁行为检测算法是当前基于警报关联的威胁行为检测技术研究中的关键问题。

3)多样化威胁引起的检测准确性问题。网络威胁行为出现的频率越来越高、类型越来越多,警报数据洪流中除包含来自于各类威胁行为导致的数据外,还用大量正常网络活动产生的数据,对系统的准确性提出了严峻的挑战。因此,如何针对多样化威胁行为类型设计准确检测算法是当前基于警报关联的威胁行为检测技术研究中的关键问题。

4)威胁模式更新引起的检测适应性问题。网络威胁行为模式会随着检测手段的升级不断进行更新,使得警报数据的分布特征和网络威胁行为的关联特点发生变化,对系统的自适应性提出了严峻挑战。因此,如何针对动态环境设计自适应检测算法是当前基于警报关联的威胁行为检测技术研究中的关键问题。

3 基于警报关联的威胁行为检测模型

许多研究者们提出了各类基于警报关联的威胁行为检测模型,不同模型的侧重点往往不同。基于对各类模型的总结分析,本节提出了一个较为全面完整的基于警报关联的威胁行为检测模型。如图 1 所示,该模型包括四个功能模块:警报预处理模块、警报约减模块、警报关联模块和威胁行为场景构建模块。警报预处理模块接收原始警报数据,将数据转化为标准格式,根据预定要求创建警报特征;警报约减模块负责去除警报数据中

的重复数据和冗余数据;警报关联模块对警报数据进行分析,挖掘具有关联关系的警报数据;威胁行为场景构建模块分析关联结果,还原威胁行为场景,提供更高层面的视角。

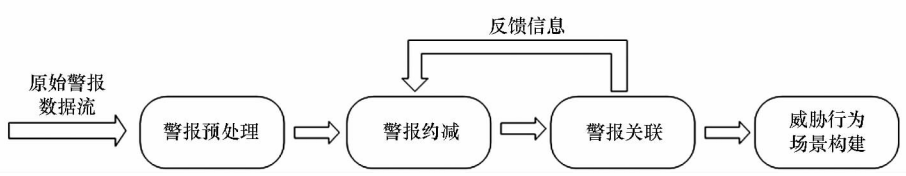


图 1　威胁行为检测模型

Fig. 1　Threat behavior detection mode

3.1　警报预处理

目前典型的安全产品包括基于主机的入侵检测系统、基于网络的入侵检测系统和防火墙等。不同类型安全产品产生的数据格式存在一定差异性,警报预处理的主要目的在于提供统一的数据格式,对警报数据的特征标准化,以进行下一步处理。

美国国防高级研究计划署(Defense Advanced Research Projects Agency, DARPA)和互联网工程任务组(Internet Engineering Task Force, IETF)的入侵检测工作组(Internet Detection Working Group, IDWG)制定了入侵检测消息交换格式(Intrusion Detection Message Exchange Format, IDMEF)[8]。IDMEF 数据模型以面向对象的形式表示入侵检测系统产生的警报数据,设计数据模型的目标是为警报提供确定的标准表达方式,并描述简单警报和复杂警报之间的关系。其中,警报被抽象成一个包含分析器、创建时间、检测编号、分析时间、源地址、目标地址、协议类型和警报级别信息的向量。大部分威胁行为检测中的预处理过程都参考该标准,处理得到的警报数据包含的信息量差异不大。

3.2　警报约减

由于入侵检测技术的不成熟导致各类安全产品暂时存在许多问题,安全产品产生的网络安全事件数据存在大量冗余和重复,而警报预处理的主要目的在于去除原始警报数据中的重复数据和冗余数据。

去除重复数据的基本思路是聚合与时间戳接近的属性值相同的原始警报,这些原始警报之间的时间差异不超过给定阈值。系统维护一个滑动窗口,每当一个新的原始警报到达后,会对该窗口进行扫描。一旦发现窗口中存在与该警报各属性值相同的警报数据,则认为这两个警报数据来自于同一安全事件,从而将它们聚合为一个超警报数据,警报时间戳设置为这两个警报中较早警报的时间戳[9-10]。

Liu 等[11]提出一种基于系统脆弱性分析的警报约减方法。通过收集目标主机系统、服务和应用程序的类型以及版本号等信息来刻画目标安全状况,将收集的警报数据与系统安全状况进行对比分析,如果能够产生威胁则保留该数据,否则认为该警报数据对系统不会产生实际的威胁效果,进行丢弃。该方法针对特定系统往往能达到较好的效果,但难以应对运行环境动态变化的系统,且系统安全状况的收集与描述需要较强的专业领域知识。

基于数据挖掘的方法借助分类、聚类及频繁项挖掘等数据挖掘技术,通过提取警报数据的各个特征、计算各个特征维度上的相似性度量并进行统计,使用相应的数据挖掘模型和方法约减冗余警报数据[12-14]。该方法在 KDD99 CUP、MIT/LL 1999、MIT/LL 2000、Defcon8 和 Defcon9 等多个数据集上被证明是有效的。但鉴于该方法普适性不强,典型数据挖掘算法的时空开销较大。

Qiao 等[7]提出一种基于反馈信息的冗余警报约减机制。该方法中,警报约减模块接收来自警报关联模块的反馈信息,记录下关联过程中几乎不与其他警报类型存在因果关联关系的警报类型,认为它们具有较高的冗余度,以此为依据过滤掉接下来待处理警报数据中冗余度较高的部分。该算法结合具体关联算法,针对性强,能够降低参与关联分析的警报数据,提高系统效率。

Hacini 等[15]提出一种在线的自适应警报约减方法,该方法包含三个部分:训练阶段、检测阶段和自适应阶段。系统在训练阶段学习正常行为数据得到正常行为模型,在检测阶段以该模型为基础进行威胁行为检测。自适应阶段采取触发机制执行,用于发现警报数据流中新威胁行为的类型。

3.3　警报关联

警报关联模块旨在找出警报之间的逻辑关

系,将疑似属于同一威胁行为的警报关联起来。按照采用技术手段的不同,典型的警报关联方法有基于因果逻辑的方法、基于场景的方法、基于相似性的方法和基于数据挖掘的方法。各种不同算法旨在挖掘警报之间的内在关系,达到检测、还原威胁行为攻击场景的目的。鉴于该模块是整个模型中最核心的部分,将在下一章节进行详细介绍分析。

3.4 威胁行为场景构建

威胁行为检测的最终目的是还原威胁行为场景。通过收集来自警报关联模块的关联分析结果,确定属于同一威胁行为的警报,从而还原威胁行为序列。同时,通过对关联结果的进一步分析,达到检测漏报警报和攻击者意图推测的目的。

吕慧颖等[16]深入分析和融合来自于多传感器的各种静态和动态安全信息,提出一种基于时空关联的网络实时威胁识别和评估方法。该方法通过模拟威胁渗透过程,构建威胁状态转移图;进而在空间维上将实时威胁与威胁状态转移图的状态属性相匹配,在时间维上将实时威胁与威胁渗透过程相关联,识别当前有效威胁及实时状态。

Zali 等[17]将规则知识库用图的形式进行表示,将关联的结果在图上进行比对分析,一旦发现某一警报对应顶点的前驱顶点无匹配警报数据,则认为出现警报漏报。同时,若某一条路径上的若干顶点均已匹配到对应警报数据,则该路径的下一顶点即为可能发生的下一异常事件,从而达到预测的目的。Jemili 等[18]将关联得到的结果构建贝叶斯概率图,以警报类型为顶点,顶点之间的边对应的数值代表一种警报之后发生另一种警报的概率。该概率图不断更新,从而达到实时预测的目的。张怡等[19]将实时 IDS 警报信息映射到攻击路径,通过计算警报关联图的转移概率对网络脆弱性进行动态分析,从而有效地反映攻击者意图。

4 警报关联方法分类

4.1 基于因果逻辑的方法

基于因果逻辑的方法假设来自于同一威胁行为的连续异常事件之间存在因果关系,后一个异常事件在前一异常事件有效的前提下进行。其基本思想是给定各种警报类型的发生需要满足的前因和发生之后造成的后果,通过匹配警报之间的前因后果对警报数据进行因果关联,从而重建网络威胁行为。

Zali 等[17]采用因果关联图模型定义警报之间的因果关系。因果关联图是一个有向无环图,图中包括两类顶点:警报标志顶点 AS 和条件顶点 Condition,AS 表示警报类型,Condition 表示警报产生的事件类型。边表示警报匹配需要满足的条件。文中通过前向队列树构建过程建立威胁行为序列,通过后向队列树构建过程来检测是否存在误报或漏报。

在 Lin 等[20]提出的实时入侵警报关联(Real-time Intrusion Alent Correlation, RIAC)中,一个警报类型被扩充为一个三元组:警报类型描述、前因事件和后果事件,通过对各个警报类型的前因与后果进行匹配,得到各个警报类型之间的因果关系和匹配需要满足的特征条件。以此为依据对警报数据进行因果关联匹配,得到关联警报序列片段,进而将这些片段连接构成完整的威胁行为。

Ramaki 等[21]提出的实时片段关联算法(Real Time Episode Correlation Algorithm, RTECA)通过维护一个因果关联矩阵表示各个警报之间的关联关系,矩阵中 i 行 j 列元素表示第 i 类警报与第 j 类警报的关联概率。RTECA 利用该因果关联矩阵对警报数据进行因果关联,同时对警报序列进行频繁项挖掘,根据得到的频繁项集结果对关联矩阵进行实时更新。

该类方法的优点在于:①只需分析威胁行为单个步骤的前因后果,无须预先定义整个威胁行为序列;②具备一定的未知威胁行为检测能力,可以识别不同警报组合形成的未知威胁行为序列。缺点在于:①只适用于各步骤之间存在明显因果关系的威胁行为,且未知威胁发现能力较弱;②关联时搜索空间较大,计算开销大,系统资源要求较高;③规则定义粒度难以控制,粒度过细会导致检测漏报率较高,粒度过粗又会导致误报率较高。

4.2 基于场景的方法

基于场景的方法的基本思想在于预先将所有已知的威胁行为抽象成规则知识,然后将待处理警报数据和已定义规则进行匹配,依据匹配结果重现网络威胁行为场景。规则知识描述了威胁行为的过程以及各个步骤需要满足的条件。

Eckmann 等[22]利用状态转移分析技术语言(State Transition Analysis Technique Language, STATL)描述威胁行为场景,每一个场景包含一个起始状态和至少一个最终状态,威胁行为是一个从起始状态到最终状态的转换序列。Morin 等[23]提出用 Chronicle 语言描述威胁行为,将一个行为场景看作是一组通过时间限制连接起来的事件

序列。

Liu 等[24]提出一种基于有限自动状态机的警报关联模型。模型中包含进程关键场景、攻击方关键场景和受攻击方关键场景三种描述视角。进程关键场景利用状态转换表示发生在攻击方与受攻击方的威胁行为序列。攻击方关键场景和受攻击方关键场景分别从攻击方和受攻击方的角度描述整个威胁行为序列。该模型能够更加直观全面地描述各类威胁行为。

基于场景的方法差异不大,主要区别在于描述威胁行为的方式不同。该类方法的优点在于:①通过多样化的场景描述语言,保持系统的灵活性;②可以通过不断更新知识库保持系统有效;③结果便于理解。其缺点十分明显:①基于已有规则难以发现新的攻击,容易被规避;②算法有一定复杂度,效率不高。

4.3　基于相似性的方法

基于相似性的方法假设来自于同一威胁行为的警报之间具有一定的相似性,其基本思想是根据警报之间的相似程度来判定是否进行警报关联,通过将警报数据的属性信息(时间戳、警报类型、地址信息等)统一抽象成向量模式,定义函数计算向量之间的距离,聚类向量以完成警报关联。基于相似性的算法的关键在于向量距离计算函数的定义。

典型方法[25-26]的过程是预先为警报的每个属性(时间戳、IP 地址、端口信息等)定义一个相似度计算函数,然后通过加权求和得到警报之间的相似度。如果该相似度超过预定阀值,则进行关联操作。主要区别在于定义属性计算函数的定义不同,文献[25]针对每一种属性特点定义一个属性相似度计算函数,文献[26]则通过定义并计算各个警报的熵来表示警报之间的相似度。文献[27]将警报的上下文信息加入到聚类过程中,在提高聚类准确性的同时有效去除冗余警报数据。

与上述方法不同的是,Lee 等[28]结合 DDoS 的警报特点,采用欧式距离作为警报之间的相似度衡量标准,提出了一种利用相似性聚类检测 DDoS 攻击的方法。Zhu 等[29]则是利用神经网络算法训练计算得到警报之间的相似性。对于新到达的待处理警报,生成已有警报之间的相似性特征向量,然后将此向量作为神经网络算法输入,根据预先的训练结果神经网络算法输出一个关联概率,得到警报类型关联图,生成威胁行为序列。同时,将此结果返回神经网络算法进行更新训练。文献[30-31]通过定义复杂的相似性函数,计算待处理警报与各威胁行为中警报的距离,以此为依据判断该警报是否属于某一威胁行为。

基于相似度的方法最大的特点就是采用定量计算方法来进行警报关联。该类方法的优点在于:①算法简单,计算开销小;②检测具有较高相似度警报数据的威胁行为(例如蠕虫攻击)时效果较好。但缺点也十分明显:①计算相似性的过程中需要大量人工设定参数;②只能针对特定攻击类型,算法通用性较差。

4.4　基于数据挖掘的方法

基于数据挖掘的方法假设来自同一网络威胁行为的警报之间具有一定的联系,其基本思想是采用数据挖掘算法来发现隐藏在数据分布之后的关联关系,根据关联关系信息重建威胁行为序列。

频繁序列挖掘是警报关联常用数据挖掘方法之一[5,32-34]。该方法认为出现在较短的时间间隔内的警报数据之间存在一定的关联关系。根据时间窗口将警报序列分解为多个子序列,然后对这些子序列进行频繁项挖掘,得到的频繁项集中的警报可认为存在关联关系。Vasilomanolakis 等[35]将事件发生的地理位置信息引入展开两维度数据分析,而葛琳等[36]提出了基于分布式幂集 Apriori 算法的多维度数据分析方法,分别挖掘各维度中的频繁项集,再进行综合关联分析。

文献[9]采用贝叶斯网络的方法挖掘警报类型之间的因果关系。方法共分为三步:首先采用贝叶斯网络学习过程得到超结构图;然后结合警报分布精简超结构图得到因果关联图,该图表示警报类型之间的因果关联概率;最后将该图添加至规则知识库对待处理警报进行检测。文献[10]将贝叶斯方法与频繁项挖掘相结合,利用贝叶斯方法计算警报间关联概率的同时,利用频繁项挖掘算法确定警报类型间的关联特征。

孙宏伟等[37]提出一种基于隐马尔可夫模型的威胁行为检测方法,根据行为模式的出现频率对其进行分类,并将行为模式类型同隐马尔可夫模型的状态联系在一起,将加窗平滑后的状态序列出现概率作为判决依据。冯学伟等[38]则是利用马尔可夫模型进行因果知识挖掘方法。该方法首先根据警报地址间的相关性对警报进行聚类分析,形成各个类簇;接着基于马尔可夫性质对每个类簇进行分析处理,挖掘警报类型之间的一步转移概率矩阵,然后对获得的转移概率矩阵进行匹配融合,构建警报之间因果知识库,基于该因果知识库研究警报的关联方法。Farhadi 等[39]则是将隐式马尔可夫链与频繁项挖掘算法结合。该算法

分为两步:第一步,采用频繁项挖掘算法提取可威胁行为序列;第二步,利用隐式马尔可夫链构建攻击概率图,从而达到通过警报数据流已有异常事件推断攻击者下一步骤的目的。

该类方法的优点在于不需要先验知识的前提下,有能力得到未知的警报类型关联关系,从而发现新的威胁行为序列。其缺点在于:①数据挖掘算法复杂度较高,计算开销大;②关联得到的结果准确性难以判断,需要结合领域知识进一步分析。

4.5 对比分析

综上所述,现阶段警报关联技术仍不够完善,多数关联技术在使用时都需要一定的限制条件。大规模复杂网络环境下,网络威胁行为类型的多样化以及威胁发生的频率越来越高,将会产生大量分布复杂的警报数据。这些数据中包含的威胁行为复杂多样,还包含大量冗余信息、误报信息等噪声数据,对警报关联技术的关联能力、关联精度、关联效率等方面提出了更高的要求。从三个方面对四类关联算法进行对比:关联能力,即该算法能够识别威胁行为类型的能力;关联精度,即该算法识别威胁行为的准确性;关联效率,与该方法的算法复杂性反相关。

如表 1 所示,基于因果逻辑的方法和基于数据挖掘的方法具有识别未知威胁行为的能力,关联能力相对较高;基于场景的方法更能与规则知识库进行匹配,关联精度相对较高;基于相似性的方法计算复杂性较小,故关联效率相对较高。

综合考虑上述因素,基于因果逻辑的算法在保证高关联精度的同时,具有一定的未知威胁行为发现能力,这是其他三种方法所不具备的。而基于数据挖掘的算法是唯一能够发现全新未知威胁行为类型的算法,其强关联能力是其他算法难以具备的。同时,计算机性能的提升使其计算开销大的问题不再成为瓶颈。因此,基于数据挖掘的方法逐渐成为主流,各种数据挖掘算法已应用到警报关联中。

表 1 关联方法优缺点对比

Tab. 1 Comparison of the methods

	关联能力	关联精度	关联效率
基于相似性的方法	低(不能因果关联)	中(依赖于相似度函数)	高(计算量小)
基于场景的方法	中(其能力依赖于知识库的更新)	高(根据已知攻击得到的专家规则)	低(多步攻击搜索空间大)
基于因果逻辑的方法	高(可以发现未知关联)	中(依赖于关联的重合度)	低(搜索空间大)
基于数据挖掘的方法	高(可以发现新规则)	低(新规则难以保证准确性)	低(计算量大)

5 威胁行为检测系统结构

威胁行为检测系统中包含两类功能模块:检测单元和关联单元,其中检测单元负责网络数据的收集分析,生成警报数据;关联单元对警报数据进行关联分析,构建威胁行为序列。根据检测单元和关联单元在系统的分布,威胁行为检测结构被分为三类:集中式结构、层次式结构和分布式结构。

5.1 集中式结构

在集中式结构中,警报关联单元接收来自全部检测单元的警报数据,并对这些数据进行集中关联分析[40-43]。如图 2 所示,所有检测单元将警报数据都汇总至中心关联单元进行统一关联处理。

集中式结构针对全网数据进行分析,能够获取完整的网络安全信息。但是,中心关联单元的失效会导致整个系统的失效。同时,网络带宽的限制会导致数据丢包和较长的处理延迟,使得系统在可靠性和可扩展性方面存在不足。因此,集中式结构往往适用于小型网络。

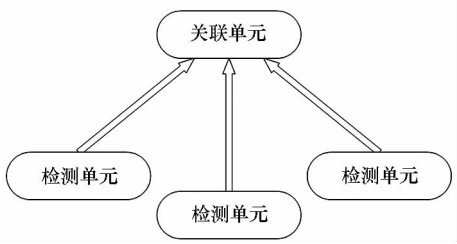


图 2 集中式结构示意图

Fig. 2 Centralized architecture

5.2 层次式结构

在层次式结构中,根据地域位置、控制级别或者软硬件环境差异等因素,网络被划分为多个级别。网络节点被分为若干组,每个小组由若干关联单元和检测单元组成,关联单元负责对该组节

点中产生的警报数据进行关联分析。关联结果被发送至上一级,重复此过程直至达到根节点,从而得到整个网络的全局视图[44-45]。如图 3 所示,整个网络被分为两个区域,每个关联单元负责所处区域内的警报数据,然后将结果向上一级关联单元传送。

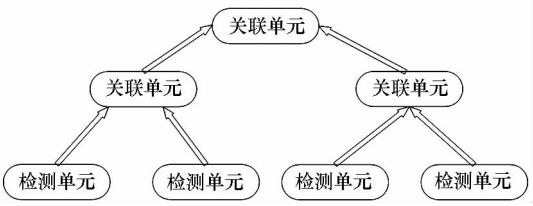


图 3　层次化结构示意图

Fig. 3　Hierarchical architecture

5.3　分布式结构

在分布式结构中,关联单元收集网络中若干检测单元的数据并进行分析,并将关联结果传送给其他相关的关联单元[46-49]。如图 4 所示,关联单元与检测单元、关联单元与关联单元之间通过交换网络进行信息交换。

分布式结构中没有中心关联单元,系统的可靠性和可扩展性有了显著提高。但分布式结构中的关联分析涉及警报数据的分派和关联结果信息的交换,使得系统的设计更加复杂,需要解决以下两个关键问题。

1)检测精度:每一个关联单元只负责对网络中部分检测单元生成的警报数据进行关联分析,因此关联精度会有一定下降。数据的传输引起通信开销,如何在通信开销与关联精度之间进行权衡是亟须解决的关键问题。

2)负载均衡:负载均衡程度直接决定着系统的实时性,任务分配不均会造成“热点”现象,导致整个系统的吞吐率下降。如何进行良好的任务划分以保证系统的负载均衡是亟须解决的关键问题。

针对上述问题,相关研究者根据应用需求提出不同的解决方案。

Mohamed 等[47]将整个网络拓扑分为不相交的若干部分,每个关联单元负责其中的一个区域,收集和分析该区域内产生的数据。各区域中关联单元通过投票投判断是否发生网络威胁行为。Khatoun 等[48]提出了一种基于 P2P 网络的 DDoS 攻击检测算法。每一个检测单元负责监控所在子网。作为 P2P 网络中子节点,各个检测单元同过分布式哈希表路由交换数据,检测可疑攻击行为,定位潜在目标。

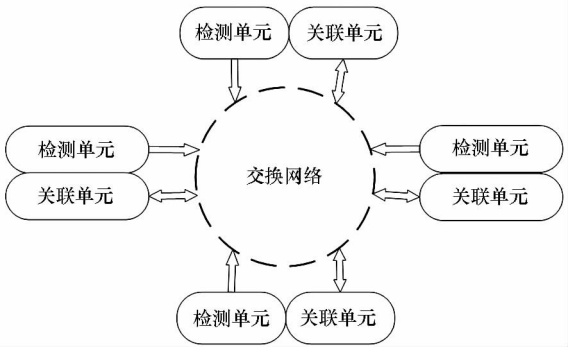


图 4　分布式结构示意图

Fig. 4　Distributed architecture

为了解决系统的负载均衡问题,Li 等[49]基于分布式入侵检测系统设计一种针对特定攻击类型的分布式路由技术。在深入分析针对 DDoS 攻击、端口扫描、蠕虫、僵尸网络四类威胁行为的特点之后,设计分布式哈希表进行警报数据的路由和关联任务的划分,在有效检测这四类威胁行为的同时保证了系统的负载均衡性。但该路由技术需要结合攻击的特点设计,因此只能针对特定攻击类型。

Rees 等[50]将威胁行为检测与分布式处理平台相结合,基于 Hadoop 开发出一套威胁行为检测系统,保证了系统良好的可扩展性和鲁棒性。Silva 等[51]则将威胁行为检测与 multi-agent 技术相结合,系统中包含多个 agent,每个 agent 运行在集群中的某个节点上,负责指定的任务(警报约减、关联等)。各个 agent 相互协作,构成整个分布式威胁行为检测系统。文献[52-53]基于博弈论提出一种分布式自主组织威胁行为检测框架,有效解决了动态网络环境中的自适应问题。

6　未来发展趋势

信息技术的不断发展使得信息安全领域对威胁行为检测准确性和实时性的要求越来越高。为进一步提高威胁行为检测的准确性,充分利用各方面资源,将网络威胁行为带来的损失降至最低,未来研究工作可以关注以下三个方面。

6.1　基于数据挖掘的威胁行为检测技术

基于数据挖掘的方法能够检测各类已知、未知威胁行为类型,其强关联能力是其他算法难以具备的。随着计算机性能的不断提升,其计算开销大的问题得到有效缓解。因此,基于数据挖掘的方法逐渐成为主流,各种数据挖掘算法应用到警报关联中。

6.2 协同检测技术

目前,网络层、系统主机、软件日志各个层面能够收集到的信息种类越来越多,数据量越来越大。通过协同检测技术,将这些信息进行全面综合分析,各类数据之间相互补充,将大大提高检测的准确性。如何设计有效的协同检测系统是未来研究的一个重要方向。

6.3 威胁行为预测技术

目前的警报关联算法主要是进行实时准确的复杂威胁行为检测,在第一时间进行响应。然而,当前威胁行为的危害越来越大,一旦发生,往往会造成无法挽回的损失。因此需要在威胁行为发生之前发现攻击者的意图,阻止威胁行为的发生。网络行为预测粒度过细会影响正常网络活动的进行,过粗则又会导致大量的漏报。如何设计可靠的威胁行为预测算法是未来研究的一个重要方向。

7 结论

本文综述了国内外基于警报关联技术的威胁行为检测技术的最新研究成果,介绍了基于警报关联的威胁行为检测模型;重点介绍了模型中核心模块——警报关联方法,分析了各类警报关联方法的原理和特点;结合实例介绍了威胁行为检测系统的三种典型结构;并基于当前研究现状,提出了对未来研究趋势的一些认识。

参考文献(References)

[1] Vasilomanolakis E, Karuppayah S, Mühlhäuser M, et al. Taxonomy and survey of collaborative intrusion detection[J]. ACM Computing Surveys, 2015, 47(4): 55.

[2] Chen T M, Abu-Nimeh S. Lessons from stuxnet [J]. Computer, 2011, 44(4): 91 – 93.

[3] 诸葛建伟, 韩心慧, 周勇林, 等. 僵尸网络研究[J]. 软件学报, 2008, 19(3): 702 – 715.
ZHUGE Jianwei, HAN Xinhui, ZHOU Yonglin, et al. Research and development of botnets [J]. Journal of Software, 2008, 19(3): 702 – 715. (in Chinese)

[4] Zuech R, Khoshgoftaar T M, Wald R. Intrusion detection and big heterogeneous data: a survey[J]. Journal of Big Data, 2015, 2(1): 1 – 41.

[5] Elshoush H T, Osman I M. Alert correlation in collaborative intelligent intrusion detection systems—a survey[J]. Applied Soft Computing, 2011, 11(7): 4349 – 4365.

[6] 胡华平, 张怡, 陈海涛, 等. 面向大规模网络的入侵检测与预警系统研究[J]. 国防科技大学学报, 2003, 25(1): 21 – 25.
HU Huaping, ZHANG Yi, CHEN Haitao, et al. The study of large scale networks intrusion detection and warning system[J]. Journal of National University of Defense Technology, 2003, 25(1): 21 – 25. (in Chinese)

[7] Qiao L B, Zhang B F, Zhao R Y, et al. Online mining of attack models in IDS alerts from network backbone by a two-stage clustering method[M]//Wang G J, Ray I, Feng D G, et al. Lecture Notes in Computer Science. Cham, Switzerland: Springer, 2013: 104 – 116.

[8] 穆成坡, 黄厚宽, 田盛丰. 入侵检测系统报警信息聚合与关联技术研究综述[J]. 计算机研究与发展, 2006, 43(1): 1 – 8.
MU Chengpo, HUANG Houkuan, TIAN Shengfeng. A survey of intrusion-detection alert aggregation and correlation techniques [J]. Journal of Computer Research & Development, 2006, 43(1): 1 – 8. (in Chinese)

[9] Ren H, Stakhanova N, Ghorbani A A. An online adaptive approach to alert correlation[C]//Proceedings of Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), 2010: 153 – 172.

[10] Kavousi F, Akbari B. A bayesian network-based approach for learning attack strategies from intrusion alerts[J]. Security & Communication Networks, 2014, 7(5): 833 – 853.

[11] Liu X J, Xiao D B. Using vulnerability analysis to model attack scenario for collaborative intrusion detection [C]// Proceedings of International Conference on Advanced Communication Technology(ICACT), 2008: 1273 – 1277.

[12] Alserhani F, Akhlaq M, Awan I U, et al. MARS: multi-stage attack recognition system[C]//Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, 2010: 753 – 759.

[13] Valeur F, Vigna G, Kruegel C, et al. Comprehensive approach to intrusion detection alert correlation[J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(3): 146 – 169.

[14] Charbonnier S, Bouchair N, Gayet P. A weighted dissimilarity index to isolate faults during alarm floods[J]. Control Engineering Practice, 2015, 45: 110 – 122.

[15] Hacini S, Guessoum Z, Cheikh M. False alarm reduction using adaptive agent-based profiling[J]. International Journal of Information Security and Privacy, 2013, 7(4): 53 – 74.

[16] 吕慧颖, 彭武, 王瑞梅, 等. 基于时空关联分析的网络实时威胁识别与评估[J]. 计算机研究与发展, 2014, 51(5): 1039 – 1049.
LYU Huiying, PENG Wu, WANG Ruimei, et al. A real-time network threat recognition and assessment method based on association analysis of time and space [J]. Journal of Computer Research and Development, 2014, 51(5): 1039 – 1049. (in Chinese)

[17] Zali Z, Hashemi M R, Saidi H. Real-time intrusion detection alert correlation and attack scenario extraction based on the prerequisite-consequence approach[J]. The ISC International Journal of Information Security, 2013, 4(2): 125 – 137.

[18] Jemili F, Zaghdoud M, Ben Ahmed M. Hybrid intrusion detection and prediction multi agent system HIDAPS [J]. International Journal of Computer Science and Information Security, 2009, 5(1): 62 – 71.

[19] 张怡, 赵凯, 来犇. 警报关联图:一种网络脆弱性量化评估的新方法[J]. 国防科技大学学报, 2012, 34(3): 109 – 112.
ZHANG Yi, ZHAO Kai, LAI Ben. Alert correlation graph:a novel method for quantitative vulnerability assessment [J]. Journal of National University of Defense Technology, 2012, 34(3): 109 – 112. (in Chinese)

[20] Lin Z W, Li S, Ma Y. Real-time intrusion alert correlation system based on prerequisites and consequence [C]// Proceedings of Wireless Communications Networking and Mobile Computing, 2010: 1 - 5.

[21] Ramaki A A, Amini M, Atani R E. RTECA: real time episode correlation algorithm for multi-step attack scenarios detection[J]. Computers & Security, 2015, 49: 206 - 219.

[22] Eckmann S T, Vigna G, Kemmerer R A. STATL: an attack language for state-based intrusion detection [J]. Journal of Computer Security, 2002, 10(1/2): 71 - 103.

[23] Morin B, Mé L, Debar H, et al. M2D2: a formal data model for IDS alert correlation [C]//Proceedings of the 5th International Conference on Recent Advances in Intrusion Detection, 2002: 115 - 137.

[24] Liu L, Zheng K F, Yang Y X. An intrusion alert correlation approach based on finite automata [C]//Proceedings of Communications and Intelligence Information Security, 2010: 80 - 83.

[25] Wang C H, Yang J M. Adaptive feature-weighted alert correlation system applicable in cloud environment [C]// Proceedings of Asia Joint Conference on Information Security, 2013: 41 - 47.

[26] Ghasemi Gol M, Ghaemi-Bafghi A. A new alert correlation framework based on entropy[C]//Proceedings of International Conference on Computer and Knowledge Engineering, 2013: 184 - 189.

[27] Shittu R, Healing A, Ghanea-Hercock R, et al. Intrusion alert prioritisation and attack detection using post-correlation analysis[J]. Computers & Security, 2015, 50: 1 - 15.

[28] Lee K, Kim J, Kwon K H, et al. DDoS attack detection method using cluster analysis [J]. Expert Systems with Applications, 2008, 34(3): 1659 - 1665.

[29] Zhu B, Ghorbani A A. Alert correlation for extracting attack strategies [J]. International Journal of Network Security, 2006, 3(3): 244 - 258.

[30] Shittu R, Healing A, Ghanea-Hercock R, et al. OutMet: a new metric for prioritising intrusion alerts using correlation and outlier analysis [C]//Proceedings of IEEE 39th Conference Local Computer Networks, 2014: 322 - 330.

[31] Daneshgar F F, Abbaspour M. Extracting fuzzy attack patterns using an online fuzzy adaptive alert correlation framework [J]. Security and Communication Networks, 2016(14): 2245 - 2260.

[32] 梅海彬, 龚俭, 张明华. 基于警报序列聚类的多步攻击模式发现研究[J]. 通信学报, 2011, 32(5): 63 - 69.
MEI Haibin, GONG Jian, ZHANG Minghua. Research on discovering multi-step attack patterns based on clustering IDS alert sequences [J]. Journal on Communications, 2011, 32(5): 63 - 69. (in Chinese)

[33] 田志宏, 张永铮, 张伟哲, 等. 基于模式挖掘和聚类分析的自适应告警关联[J]. 计算机研究与发展, 2009, 46(8): 1304 - 1315.
TIAN Zhihong, ZHANG Yongzheng, ZHANG Weizhe, et al. An adaptive alert correlation method based on pattern mining and clustering analysis[J]. Journal of Computer Research & Development, 2009, 46(8): 1304 - 1315. (in Chinese)

[34] Paredes-Oliva I, Dimitropoulos X, Molina M, et al. Automating root-cause analysis of network anomalies using frequent itemset mining [J]. ACM SIGCOMM Computer Communication Review, 2011, 41(4): 467 - 468.

[35] Vasilomanolakis E, Karuppayah S, Kikiras P, et al. A honeypot-driven cyber incident monitor: lessons learned and steps ahead [C]//Proceedings of the 8th International Conference on Security of Information and Networks, 2015: 158 - 164.

[36] 葛琳, 季新生, 江涛. 基于关联规则的网络信息内容安全事件发现及其 Map-Reduce 实现[J]. 电子与信息学报, 2014, 36(8): 1831 - 1837.
GE Lin, JI Xinsheng, JIANG Tao. Discovery of network information content security incidents based on association rules and its implementation in Map-Reduce [J]. Journal of Electronics & Information Technology, 2014, 36(8): 1831 - 1837. (in Chinese)

[37] 孙宏伟, 田新广, 邹涛, 等. 基于隐马尔可夫模型的 IDS 程序行为异常检测[J]. 国防科技大学学报, 2003, 25(5): 63 - 67.
SUN Hongwei, TIAN Xinguang, ZOU Tao, et al. Anomaly detection of the program behaviors for IDS based on hidden Markov models[J]. Journal of National University of Defense Technology, 2003, 25(5): 63 - 67. (in Chinese)

[38] 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.
FENG Xuewei, WANG Dongxia, HUANG Minhuan, et al. A mining approach for causal knowledge in alert correlating based on the Markov property [J]. Journal of Computer Research & Development, 2014, 51(11): 2493 - 2504. (in Chinese)

[39] Farhadi H, Amirhaeri M, Khansari M, et al. Alert correlation and prediction using data mining and HMM [J]. The ISC Journal of Information Security, 2011, 3(2): 77 - 101.

[40] Sadighian A, Fernandez J M, Lemay A, et al. ONTIDS: a highly flexible context-aware and ontology-based alert correlation framework [C]//Proceedings of Revised Selected Papers of the 6th International Symposium on Foundations and Practice of Security, 2014: 161 - 177.

[41] Yu J, Reddy Y V R, Selliah S, et al. TRINETR: an intrusion detection alert management systems [C]// Proceedings of International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2004: 235 - 240.

[42] Amiri F, Gharaee H, Enayati A R. A complete operational architecture of alert correlation [C]//Proceedings of International Conference on Computational Aspects of Social Networks, 2011: 243 - 248.

[43] Elshoush H T, Osman I M. An improved framework for intrusion alert correlation [C]//Proceedings of the World Congress on Engineering, 2012, 1: 1 - 6.

[44] Tian D H, Hu C Z, Qi Y, et al. Hierarchical distributed alert correlation model [C]//Proceedings of International Conference on Information Assurance and Security, 2009: 765 - 768.

[45] Huang S Y, Huang Y, Suri N. Event pattern discovery on IDS traces of cloud services[C]//Proceedings of IEEE Fourth International Conference on Big Data and Cloud Computing, 2014: 25 - 32.

[46] Elshoush H T I. An innovative framework for collaborative intrusion alert correlation [C]//Proceedings of Science and Information Conference, 2014: 607 - 614.

[47] Mohamed A A, Basir O. Fusion based approach for

distributed alarm correlation in computer networks [C]// Proceedings of International Conference on Communication Software and Networks, 2010: 318 – 324.

[48] Khatoun R, Doyen G, Gaïti D, et al. Decentralized alerts correlation approach for DDoS intrusion detection [C]// Proceedings of New Technologies, Mobility and Security, 2008: 1 – 5.

[49] Li Z C, Chen Y, Beach A. Towards scalable and robust distributed intrusion alert fusion with good load balancing[C]// Proceedings of SIGCOMM Workshop on Large-scale Attack Defense, 2006: 115 – 122.

[50] Rees J. Distributed multistage alert correlation architecture based on Hadoop[C]//Proceedings of International Carnahan Conference on Security Technology, 2015: 147 – 152.

[51] da Silva Thiago V, Rego P A L, de Souza J N. Multi-agents architecture for distributed intrusion detection [C]// Proceedings of the Ninth Advanced International Conference on Telecommunications, 2015: 50 – 55.

[52] Bartos K, Rehak M, Svoboda M. Self-organized collaboration of distributed IDS sensors [M]//Flegel U, Markatos E, Robertson W. Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, Heidelberg: Springer, 2012: 214 – 231.

[53] Bartos K, Rehak M. Distributed self-organized collaboration of autonomous IDS sensors[C]//Proceedings of the 6th IFIP WG 6.6 International Autonomous Infrastructure, Management, and Security Conference on Dependable Networks and Services, 2012: 113 – 117.

(上接第49页)

[9] 施闯, 赵齐乐, 李敏, 等. 北斗卫星导航系统的精密定轨与定位研究[J]. 中国科学: 地球科学, 2012, 42(6): 854 – 861.
SHI Chuang, ZHAO Qile, LI Min, et al. Precise orbit determination of BeiDou satellites with precise positioning[J]. Scientia Sinica (Terrae), 2012, 42(6): 854 – 861. (in Chinese)

[10] 刘福声, 罗鹏飞. 统计信号处理[M]. 长沙: 国防科技大学出版社, 1999: 194 – 195.
LIU Fusheng, LUO Pengfei. Statistical signal processing[M]. Changsha: National University of Defense Technology Press, 1999: 194 – 195. (in Chinese)

[11] 阳仁贵, 袁运斌, 欧吉坤. 相对实时查分技术应用于飞行器交会对接研究[J]. 中国科学:物理学 力学 天文学, 2010, 40(5): 651 – 657.
YANG Rengui, YUAN Yunbin, OU Jikun. Real-time GNSS carrier phase differential technique for spacecraft rendezvous and docking [J]. Scientia Sinica (Physica, Mechanica & Astronomica), 2010, 40(5): 651 – 657. (in Chinese)

[12] 李金龙. 北斗/GPS 多频实时精密定位理论与算法[J]. 测绘学报, 2015, 44(11): 1297.
LI Jinlong. BDS/GPS multi-frequency real-time kinematic positioning theory and algorithms [J]. Acta Geodaetica et Cartographica Sinica, 2015, 44(11): 1297. (in Chinese)

[13] Ye S R, Chen D Z, Liu Y Y, et al. Carrier phase multipath mitigation for BeiDou navigation satellite system [J]. GPS Solution, 2015, 19(4): 545 – 557.

[14] Zhao C Y, Zhang M J, Wang H B, et al. Analysis on the long-term dynamical evolution of the inclined geosynchronous orbits in the Chinese BeiDou navigation system[J]. Advances in Space Research, 2015, 56(3): 377 – 387.

[15] Li J L, Yang Y X, Xu J Y, et al. GNSS multi-carrier fast partial ambiguity resolution strategy tested with real BDS/GPS dual-and triple-frequency observations [J]. GPS Solution, 2015, 19(1): 5 – 13.

[16] Han C H, Yang Y X, Cai Z W, et al. BeiDou navigation satellite system and its time scales [J]. Metrologia, 2011, 48(4): S213 – S218.