一种基于多源异构传感器的网络安全态势感知模型 *

张 焱[1], 郭世泽[2], 黄曙光[1], 汪永益[1]
(1. 电子工程学院 网络系, 合肥 230037; 2. 北京邮电大学 计算机学院, 北京 100876)

摘 要: 为了分析安全事件对网络的影响,准确、全面地评估系统的安全态势,并迅速找出系统中的最薄弱环节,提出一种基于多源异构传感器的网络安全态势评估模型。首先,运用改进的 DS 融合规则结合 AHP 算法对多传感器提交的安全数据进行初步融合;然后,针对可能造成的漏报问题,配合预定义的安全策略进行全局融合,得到整个网络当前的安全态势。通过对实验网络的分析表明,提出的方法符合实际应用,评估结果准确、有效,有助于更好地调整系统安全策略。

关键词: 传感器; 安全数据; 评估
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2011)01-0286-04
doi:10.3969/j.issn.1001-3695.2011.01.079

Novel multi-heterogeneous sensor based network security situation awareness model

ZHANG Yan[1], GUO Shi-ze[2], HUANG Shu-guang[1], WANG Yong-yi[1]
(1. *Dept. of Network, Electronic Engineering Institute, Hefei* 230037, *China*; 2. *School of Computer Science, Beijing University of Posts & Telecommunications, Beijing* 100876, *China*)

Abstract: In order to analyze the influence of security incidents on a network system and accurately evaluate system security, this paper proposed a new network security situation awareness model based on multi-heterogeneous sensors. Firstly, by using improved DS fusion rules and combining with AHP algorithm, it fused security data submitted from different sources. Secondly, to deal with the potential missing report problem, it performed global fusion using predefined security policy so as to get the current security situation of the whole network. The evaluation of a simulated network indicates that this approach is suitable for real network environment, and the evaluation result is precise and efficient.

Key words: sensor; security data; assessment

0 引言

随着计算机及网络技术的发展,面临的安全威胁也在不断加剧,网络安全态势感知(network security situation awareness, NSSA)作为觉察(perception)、理解(comprehension)、预测(projection)网络安全状态的重要手段逐渐成为信息安全领域研究的热点问题。目前,针对 NSSA 的研究大部分集中于架构模型,例如:文献[1]提出的多传感器数据融合架构;文献[2]提出的基于网络流量的 VisFlowConnect-IP 架构以及文献[3]提出的分布式模型架构。这些研究大都基于数据融合技术,解决了多源异构网络安全设备的管理及维护问题。但是在实际操作中,告警量过载(alert overload)、告警冲突(alert conflict)及告警误报率(false positive)过高等问题制约了 NSSA 系统的应用。

针对这些问题,报警记录分析技术被提出并受到重视,其目的在于融合重复报警,关联不同阶段的报警,形成更高层次和精练的信息给后台管理者。文献[4]提出一种关联分析(correlation analysis)方法,侧重解决数据简化问题,以减轻安全设备产生的海量告警信息给管理造成的负担。文献[5]提出一种基于相似度计算的概率关联方法,根据报警属性的相似度进行聚合与关联。文献[6]提出了从被保护网络系统的角度来关联报警信息。也有部分研究针对 DDoS 和多步骤攻击进行分析[7,8],试图从大量报警和多来源的报警信息中提炼攻击步骤,以重现攻击场景(attack scenario)。

本文基于报警记录分析技术,提出了一种网络安全态势评估模型 HNSMS,着重解决报警冲突问题。首先,基于改进的 DS/AHP 算法,利用不同安全设备对不同形态攻击所具有的不同可信程度和权重信息,对各种安全设备上报的报警记录进行初步融合;然后,针对可能造成的漏报问题,配合预定义的安全策略进行全局融合;最后,通过模拟案例的分析表明,本文提出的方法不仅能够提供管理者当前网络真实的安全状况,还有助于适时地调整系统安全策略,提高网络整体安全性。

收稿日期: 2011-06-12; **修回日期**: 2011-0-17 **基金项目**: 国家自然科学基金资助项目(61070208)

作者简介:张焱(1983-),男,博士,主要研究方向为计算机网络、信息安全(eeijack@163.com);郭世泽(1969-),男,博士,研究员,主要研究方向为信息安全、密码学;黄曙光(1960-),男,硕士,教授,主要研究方向为计算机体系结构、信息安全;汪永益(1969-),男,硕士,教授,主要研究领域为信息安全.

1　相关研究

1.1　层次分析法

层次分析法(analytic hierarchy process,AHP)是美国运筹学家 Saaty 教授于 20 世纪 70 年代中期提出的一种多目标决策方法,主要通过对问题从不同层面进行分解达到将复杂问题系统化的目的。AHP 一般应用于不确定情况以及具有多个评估准则的决策问题,利用有组织的系统架构,建立具有相互影响关系的分层架构,对复杂的问题或不确定的风险作出最有效的决策。

由于通过定性与定量相结合的方式处理决策因素,以及灵活简洁等优点,AHP 迅速在能源系统分析、城市规划、经济管理、科研评价等诸多领域得到了应用。近年来,许多研究试图将 AHP 应用于信息安全领域,取得了一些成果。例如,文献[9]将 AHP 方法运用于网络安全态势感知,提出了一种层次化安全威胁态势量化评估模型。该模型基于 IDS 的报警发生频率、报警严重性及其网络带宽耗用情况,对服务、主机本身的重要性因子进行加权,计算服务、主机以及整个网络系统的威胁指数,进而分析安全威胁态势,得到了较好的实验效果。文献[10]提出了一种网络安全态势感知的指标体系,从应用层—主机层—网络层三个层次对网络安全的相关信息进行分类、标准化和系统化。

但是,以上采用的 AHP 方法还存在一些问题。比如:AHP 无法解决不确定性问题,使得评估结果较实际问题产生误差[11];当选择的方案间非常接近时,评估结果可能产生显著差异[12];当层级结构增加时,计算过程复杂度迅速增加等。

1.2　DS 证据理论(DS evidence theory)

DS 证据理论是由 Dempster 于 1967 年首先提出,并由他的学生 Shafer 于 1976 年进一步发展起来的一种不精确推理理论,也称为 Dempster-Shafer 证据理论。在决策分析领域中有许多无法充分表达具有确定性的重要决策信息,于是便产生不确定问题,由于缺乏足够决策信息无法推测先验概率,因此会影响贝叶斯定理的推理效率。DS 证据理论被广泛运用的主要原因是推理的过程比较符合人类思考模式的推理与决策过程,同时又可将所有可能的证据组合在一起,通过对证据的支持产生信任函数,最后对命题进行合适推理与判断,因此 DS 证据理论比传统的概率理论更适用于处理未知性与不确定性的问题。

在使用 DS 融合规则前,首先需要定义目标框架 Θ,即欲理解的事件:

$$A\subseteq\Theta \text{ 且 } A\neq\varnothing,\text{有 } m(A)>0 \tag{1}$$

其中,A 为鉴别框架中的元素。接着利用 BPA(basic probability assignment)公式分配不同传感器对不同事件描述的信任程度。框架中的 BPA 函数 m 是一个[0,1]之间的常数,且满足下列条件:

$$\begin{gathered} m:2^{\Theta}\rightarrow[0,1] \\ m(\varnothing)=0 \\ m(A)\geqslant 0,\forall A\in 2^{\Theta} \\ \sum\{m(A)\mid A\in 2^{\Theta}\}=1 \end{gathered} \tag{2}$$

不同命题的证据具有不同概率分配函数,Shafer 提出通过正交求和的方法来合并各相关证据的 BPA,主要目的在于逐步缩小不确定区间,化解证据间的矛盾,得到综合各证据影响力的融合结果。DS 证据合并法则可以表示

$$m_x\oplus m_y(A)=\frac{\sum\limits_{B\cap C=A}m_x(B)m_y(C)}{1-\sum\limits_{B\cap C=\varnothing}m_x(B)m_y(C)}=\frac{\sum\limits_{B\cap C=A}m_x(B)m_y(C)}{1-K_{\text{Conflict}}}$$
$$K_{\text{Conflict}}=\sum_{B\cap C=\varnothing}m_x(B)m_y(C) \tag{3}$$

在 DS 证据合并法则中冲突系数 K_{Conflict} 是一种正规化常数,主要用于衡量同一假设空间中各证据间的矛盾程度,并且避免概率值直接分配给空集合$\varnothing$,K_{Conflict} 的范围介于 $0\leqslant K_{\text{Conflict}}\leqslant 1$。$K_{\text{Conflict}}$ 值越大代表证据间的冲突越激烈,值越小代表证据是一致的或部分一致。

2　改进的 DS/AHP 算法

DS 证据理论中各证据彼此冲突矛盾的情况是无法避免的,合并时必须评估 K_{Conflict} 数值大小,一旦 K_{Conflict} 接近于 1,则有可能产生不合理结果,进而影响到 DS/AHP 的结果,因此本文将传统 DS 证据理论合并规则进行改进,有效降低 K_{Conflict} 并减少不合理结果发生的概率。

2.1　改进的 DS 证据合并规则

目前 DS 证据理论的应用主要受制于 K_{Conflict} 值范围的大小,K_{Conflict} 能够使证据合并的结果产生不合理情况,直接影响到 DS/AHP 方案的结果与效率。为了处理 K_{Conflict} 的问题,本文提出的 DS 证据理论合并规则,必须同时满足既能够降低 K_{Conflict} 又符合直觉上的合理性,同时还要降低整体合并次数。

Liu 等人[13]提出了一种基于平均法的 DS 证据合并规则:

$$\bar{m}(A)=\frac{1}{n}\sum_{1\leqslant i\leqslant n}m_i(A) \tag{4}$$

其中:n 为准则数目。

本文将该合并规则进行改进,达到既可以保持结果的合理性,又能够解决 K_{Conflict} 数值过高的问题。改进后的合并规则为

$$\bar{m}\cap(A)=\sum_{B\cap C=A}\bar{m}_1(B)\cdot\bar{m}_2(C),\forall A\subseteq\Theta,A\neq\Phi \tag{5}$$

$$\bar{m}\cap(\Phi)=\sum_{B\cap C=\Phi}\bar{m}_1(B)-\bar{m}_2(C),K_{\text{Conflict}}=\bar{m}\cap(\Phi) \tag{6}$$

$$m_{\text{new}}(A)=\frac{\bar{m}\cap(A)}{1-\bar{m}\cap(\Phi)},\forall A\subseteq\Theta,A\neq\Phi \tag{7}$$

2.2　算法流程

为了详细说明算法过程,图 1 给出了本文的 DS/AHP 算法流程图。

a)确定问题的总体目标,说明各种可行的解决方案,列出总体目标的影响因素。至上而下建立层级架构,评估影响因素对方案的影响力。

b)建立各层级间的比较矩阵,求解各层级因素的特征向量值与最大特征向量。

c)以 C. R. 检验各层级因素的特征向量值与架构是否符合一致性,若不符合则重新评估影响因素。

d)取出符合 C. R. 检验准则的特征向量值。

e)将所有方案构成一个鉴别框架,依据不同特性的准则对方案进行分类与分级,决策者依据判断尺度对不同准则下的各方案偏好程度进行打分,形成分类方案树。

f)利用式(8)构造初始比较矩阵。

$$A_s=\begin{bmatrix}1 & 0 & \cdots & 0 & a_1\\ 0 & 1 & 0 & 1 & a_2\\ \cdots & 0 & \ddots & 0 & \cdots\\ 0 & \cdots & 0 & 1 & a_d\\ \frac{1}{a_1} & \frac{1}{a_2} & \cdots & \frac{1}{a_i} & 1\end{bmatrix}\cdot\ d=1,2,\cdots,d \tag{8}$$

其中:A_x 为某一评估准则,a_d 为该准则下各方案的优势程度。

g)利用式(9)(10)得到正规化后比较矩阵的特征向量值,反复进行 f)~g)计算所有准则下方案的特征向量值。

$$A_x=\begin{bmatrix}1 & 0 & \cdots & 0 & P_k a_1\\ 0 & 1 & 0 & \cdots & P_k a_2\\ \cdots & 0 & \ddots & 0 & \cdots\\ 0 & \cdots & 0 & 1 & P_k a_d\\ \frac{1}{P_k a_1} & \frac{1}{P_k a_2} & \cdots & \frac{1}{P_k a_i} & 1\end{bmatrix},d=1,2,\cdots \tag{9}$$

其中:p_k 为某一评估准则的相对向量权重。

$$x_d=\frac{P_k a_j}{\sum_{i=1}^{d}P_k a_i+\sqrt{d}},d=1,2,\cdots$$

$$X_\Theta=\frac{\sqrt{d}}{\sum_{i=1}^{d}P_k a_i=\sqrt{d}} \tag{10}$$

其中:d 为分类树下某评估准则的方案数目。

h)利用式 e)~g)对所有准则方案的特征向量值进行合并,求得对该目标所有方案的 BPA。

i)以 K_{Conflict} 检验各证据合并所产生的结果是否符合一致性,若不符合则重新建立分类方案树。

j)利用式(11)(12)求得信任函数 Bel 与似真函数 Pl,并且建立信任区间。

$$\text{Bel}(A_i)=\sum_{B\subseteq A_i}m_x(B) \tag{11}$$

$$Pl(A_i)=\sum_{B\cap A_i\neq\varnothing}m_x(B)=1-\text{Bel}(A_i^c) \tag{12}$$

k)针对 Bel 以及 Bel 与 Pl 之间差距进行排序,Bel 数值越高,表示该方案获得使用者支持的程度较高,差距数值越低,则表示为较好的选择方案,因此使用者在选择方案时选择需 Bel 数值较高、Bel 与 Pl 之间差距数值较低的为最佳选择方案。

3　网络安全态势感知模型

为了解决多源异构网络传感器环境下的报警冲突问题,本文将改进的 DS/AHP 算法应用到网络安全态势感知中,提出一种异构网络传感器管理服务框架(heterogeneous network sensors management service,HNSMS),并根据态势感知的三项层级结构(perception,comprehension,projection)构造出九个模块,如图 2 所示。

HNSMS 架构基于改进的 DS/AHP 算法,利用管理者设置的报警置信度、权重以及反馈信息,着重解决在异构网络安全传感器中产生的报警冲突问题,让后端管理者得到最新的系统状态,以便作出合适回应。

系统架构主要包含九个模块:

a)预处理(pre-processing)。负责搜集来自不同网络传感器的报警信息,并转换成统一格式,使其能符合 HSSMS 架构的处理流程。

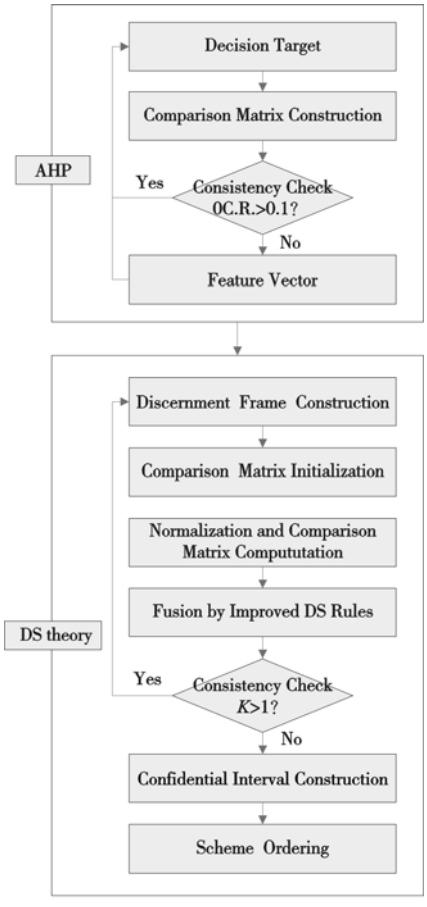

图1　改进的DS/AHP算法流程图

b)置信度设置(confidence assign)。不同的网络传感器对于不同类型的攻击具有不同的可信程度,因此需要通过专家的经验知识来设置,系统运行时也可以根据需要进行微调。

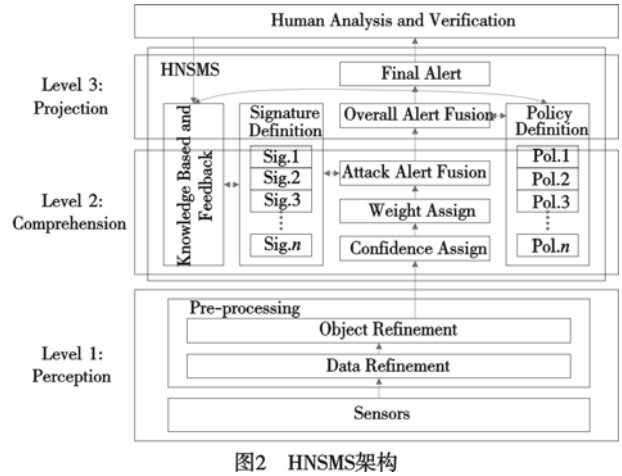

图2　HNSMS架构

c)权重设置(weight assign)。除了不同的网络传感器对于不同类型的攻击具有不同的可信程度,不同的网络传感器对相同类型攻击的信任度也不尽相同。举例来说,假设有两项安全系统 O_1 及 O_2。对于攻击 A_k,O_1 的可信度为 0.02,而 O_2 的可信度为 0.7。如果 O_1 对攻击 A_k 的检测能力非常弱,就可以通过权重的设置来改善结果。因此可以设置 O_1 对攻击 A_k 检测的权重值为 $w_1^k=0.2$,O_2 权重值为 $w_2^k=1$。

d)攻击特征定义(signature definition)。定义已知的攻击特征。

e)安全策略定义(policy definition)。并非所有攻击都能通过单一攻击特征来发现,可以利用时间段或攻击次数等辅助

信息来判别。

f)知识库及反馈(knowledge base and feedback)。储存各网络传感器的相关信息,同时包含可进行人为调整的反馈机制。

g)攻击报警融合(attack alert fusion)。基于量化的权重以及可信度等信息,采用改进的 DS 证据合并规则,对多源的报警信息进行融合,以解决报警冲突问题。

h)全局报警融合(overall alert fusion)。针对无法用单一攻击特征所能识别的攻击,配合特定的安全策略,计算联合事件强度,依据这一数值大小评估整体安全性。

i)最终报警(final alerts)。最终的报警按照重要性等级(severity level)进行分类,并通过自动化控制界面,事件快速反应界面、实时监控界面等反馈给管理者。后台管理者可依据网络当前安全态势的重要性等级来作最适当的处理。

异构网络传感器管理服务的九项模块的流程说明如图 3 所示。从各种不同的网络传感器所转送的报警经过预处理后成为统一格式,设置了置信度及权重后进行攻击报警融合。若为紧急报警,则直接报告网管人员;否则继续进行安全策略的确认,即进行全局的报警融合。最终得到的报警通过后台管理人员判别后进行反馈,即对知识库中的内容进行微调。

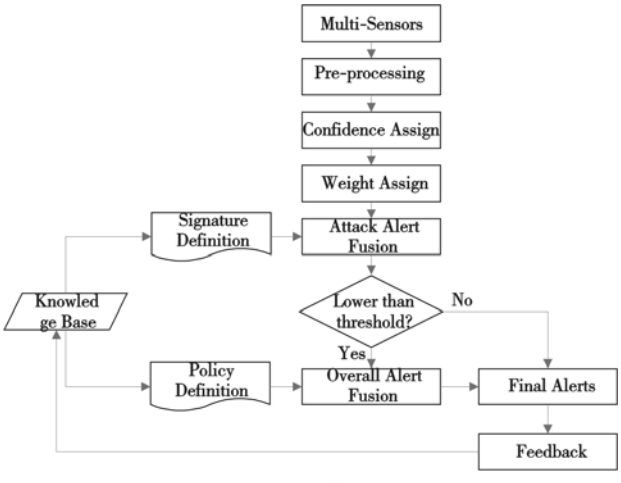

图3　HNSMS报警处理流程

4　实验结果及分析

为了检验本文 HNSMS 模型的效果,本文设置多重传感器环境的态势(图 4)。在模拟的网络环境中,部署了四种不同传感器,首先在互联网入口设置防火墙(firewall),接着在防火墙之后配置网络型入侵检测系统(network intrusion detection system),最后在用户端计算机上安装主机型入侵检测系统(host intrusion detection system)及杀毒软件(Anti-Viruses),通过这四项安全设备来保护并监控网络状况。

实验中,通过远程入侵行为的分析来检验 HNSMS 系统的效果。当入侵者通过攻击特定主机访问内部网络时,可能会尝试使用主机中多个用户的账号密码进行登录。此时,登录失败的事件将导致网络型入侵检测系统 N-IDS 和主机型入侵检测系统 H-IDS 发出报警,防火墙及防毒软件则不会报警。网络型入侵检测系统及主机型入侵检测系统发出报警后,将该报警信息传送到 HNSMS 服务器进行分析。

因为不同的网络传感器对于不同的安全事件具有不同的

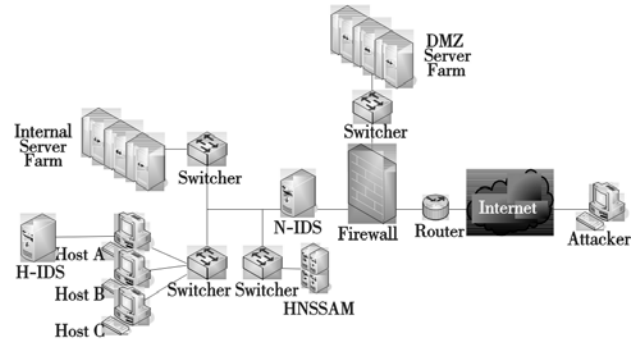

图4　实验网络环境配置图

防护重点,而系统中四项安全设备中的两项发出了报警,另两项却未发出报警,因此产生了冲突。HNSMS 对这些报警信息进行整合处理,步骤如下:

a)进行事件分析时首先要参照引用知识库中的信息,即给定置信度及权重,进行攻击报警的融合。表 1 给出了各网络传感器的置信度及权重。

表 1　各传感器的置信度及权重分配

Sid	Sig_id	Confidence	Weight
1	4	0.01	1
2	4	0.2	0.5
3	4	0.4	1
4	4	0.01	1

b)融合这两项安全设备的置信度来判断系统是否处于安全状态。通过改进的 DS 融合规则,配合其安全设备的置信度及权重值,代入式(7),可得式(13)攻击警讯融合的计算式。

$$m_{23}(\{A_4\}) = \frac{0.2^{0.5} \times 0.4^{1}}{0.2^{0.5} \times 0.4^{1} + 0.8^{0.5} \times 0.6^{1}} = 0.25 \qquad (13)$$

c)对攻击报警进行融合后,假设融合的置信度数值偏低(阈值可视情况设置),便可以说此时的系统处于正常状态。

d)从这一案例来看,结果与事实不符,原因是当合法用户因错误键入账号密码而产生登录失败也属于正常行为,因此仅凭单一时间点的报警是无法判别的。

e)由于经过攻击报警融合未发现任何异常,下一步进入全局报警模块。全局报警融合是利用辅助的信息来判断是否处于安全状态,其中包括“登录失败次数”“攻击间隔时间”“用户”及“主机”等四项信息。在进行事件分析时利用知识库储存的评估准则,进行全局报警融合得到式(14)全局报警融合计算式。

$$\frac{4 \times 1 + 4 \times (-0.5) + 4 \times 0.5 + 4 \times 0.75}{1 + (-0.5) + 0.5 + 0.75} = 4 \qquad (14)$$

f)经过全局报警融合后,得到的安全态势数值偏高,因此可以确定此时的系统处于异常状态,反馈给管理人员。

g)得到了当前的网络安全态势,后台管理者就可以对知识库中的内容进行修正调整,以便下次对攻击融合时,能够得到更精确的结果。

通过以上分析可以看出,攻击者发动登录验证攻击后,仅有 N-IDS、H-IDS 两项安全设备发出报警。如果不经过 HNSMS 的攻击报警融合,把“登录失败”消息直接回馈给后台管理人员,管理人员通常会把这些事件视为无效报警。但是通过 HNSMS 框架的多级报警融合后,可以成功地发现攻击行为,有效帮助管理人员及时调整安全策略。

(下转第 293 页)

one with the earliest receipt time.
14　return Mes and Sig　}

节点 P 所发送的信息 Mes_i,为其添加 ACK 属性,当接收到 Mes_i 的应答信息后标记为 ACKed。协商策略确保每个发送的消息应该并且只接收到一次应答消息。节点如果发送的所有消息都得到了应答并且节点接收到的信息也都发送了应答消息,则节点状态为终止,否则状态为活动。当节点 P 接收到一个消息 m,如果 m 是数据消息则使用基本策略计算其应该回复的数据消息 Mes,如果 m 是应答信息则标记其相应的先前发送的消息 Mes_i 的 ACK 属性为 ACKed。Sig 为 P 将要发送的应答信息集合,节点 P 已经接收到数据消息但还没有回复应答的信息存放在集合 Rev 中,如果节点 P 发送的消息都已回复 ACKed 或者 P 是协商发起者,则 Rev 中的所有消息都需要回复 ACK 信息,否则需要去除最早接收到的那个数据消息。最后发送数据消息集合 Mes 和应答信息集合 Sig。完整协商策略同样具备安全性和完备性。

3　结束语

自动信任协商技术解决了跨多安全域隐私保护、信任建立等问题,成为一个崭新的研究领域,其研究和应用在国际上备受关注。本文在整理、归纳现有文献中所出现的概念、定义的基础上,定义了两个以上参与方时信任协商的策略语言、安全披露序列、完整协商策略,讨论了协商策略的安全性、完备性等关键概念。本文的协商策略是一种积极策略,披露所有可满足访问控制策略保护的信任证。任何一种新技术从它的诞生、发展到被广泛接受都需要进行不断的探索和实验,随着物联网与云计算的飞速发展,对可信协作的需求越来越迫切,需要对信任协商技术继续展开更深入的研究。

参考文献:

[1] WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated trust negotiation[C]//DARPA Information Survivability Conference and Exposition. New York: IEEE Press,2000:88-102.

[2] LI N H, MITCHELL J C, WINSBOROUGH W H. Design of a role-based trust management framework[C]//Proc of the 2002 IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society Press, 2002:114-130.

[3] LI N H, WINSBOROUGH W H, MITCHELL J C. Distributed credential chain discovery in trust management[C]//Proc of the 8th ACM Conference. 2001:156-165.

[4] SEAMONS K E, WINSLETT M, YU T. *et al*. Protecting privacy during on-line trust negotiation[C]//Proc of the 2nd Workshop on Privacy Enhancing Technologies. Berlin: Springer-Verlag, 2002.

[5] YU T, WINSLETT M. SEAMONS K E, *et al*. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation[J]. ACM Trans on Information and System Security, 2003, 6(1).

[6] Yu T. Automated trust establishment in open systems [D]. Illinois: University of Illinois, 2003.

[7] De TREVILLE J. Binder, a logic-based security language[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2002.

[8] SEAMONS K E, WINSLETT M, YU T, *et al*. Limiting the disclosure of access control policies during automated trust negotiation [C]// Network and Distributed System Security Symposium. 2001.

[9] DIJKSTRA E W, SCHOLTEN C S. Termination detection for diffusing computations[J]. Information Processing Letters, 1980, 11(1):134-145.

(上接第 289 页)

5　结束语

本文分析了目前存在的网络安全态势评估算法,提出了一种基于多源异构传感器的网络安全态势评估模型及其实现方法。根据态势感知模型实现了相应的原型系统,通过对实验网络环境的分析发现,本文提出的方法不仅能够提供管理者当前网络真实的安全状况,还有助于适时地调整系统安全策略,提高网络整体安全性。

参考文献:

[1] 赖积保,王颖,王慧强,等.基于多源异构传感器的网络安全态势感知系统结构研究[J].计算机科学,2011,38(3):144-149.

[2] YIN Xiao-xin, YURCIK W, SLAGELL A, The design of visflowconnect-IP: a link analysis system for IP security situational awareness [C]//Proc of the 3rd IEEE International Workshop on Information Assurance (IWIA). 2005:141-153.

[3] BATSELL S G, RAO N S, SHANKAR M. Distributed intrusion detection and attack containment for organizational cyber security[EB/OL]. http://www. ioc. oml. gov/projects/documents/containment. pdf, 2005.

[4] LEE S, CHUNG B, KIM H, *et al*. Real-time analysis of intrusion detection alerts via correlation[J]. Computers & Security, 2006, 25(3):169-183.

[5] VALDES A, SLONNER K. Probabilistic alert correlation[C]//Proc of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001). London: Springer Verlag, 2001:54-68.

[6] MU C, HUANG H, TIAN S. Intrusion detection alert verification based on multilevel fuzzy comprehensive evaluation[C]//Proc of the 2005 International Conference on Computational Intelligence and Security. Berlin: Springer-Verlag, 2005:9-16.

[7] QIN X, LEE W. Discovering novel attack strategies from INFOSEC alerts[C]//Proc of the 9th European Symposium on Research in Computer Security. [S. l.]:Sophia Antipolis, 2004:439-456.

[8] STEVEN C, ULF L, MARTIN W F. Modeling multistep cyber attacks for scenario recognition[C]//Proc of the 3rd DARPA Information Survivability Conference and Exposition. 2003:284-292.

[9] 陈秀真,郑庆华,管晓宏,等.层次化网络安全威胁态势量化评估方法[J].软件学报,2006,17(04):885-897.

[10] 王娟,张凤荔,傅翀,等.网络态势感知中的指标体系研究[J].计算机应用,2007,27(8):1907-1909.

[11] BELTON V, GEAR A E. On a shortcoming of Saaty's method of analytic hierarchies[J]. Omega, 1983, 11:227-230.

[12] DYE C Y. Joint pricing and ordering policy for a deteriorating inventory with partial backlogging[J]. Omega, 2007, 35(2):184-189.

[13] LIU Y S, HUANG G S. A new combination rule of evidence theory based on consensus[C]//Proc of International Conference on Machine Learning and Cybernetics. 2005:18-21.