·安全技术· 文章编号：1000—3428(2013)04—0158—07 文献标识码：A 中图分类号：TP393.08

基于情景感知的网络安全风险评估模型与方法

威 溟，王 艳，李千目
(南京理工大学计算机学院，南京 210094)

摘 要：现有情景感知框架对网络安全风险评估没有精确的量化方法，为此，结合DS证据理论和协商目标风险分析系统，提出一种基于情景感知框架的网络安全风险评估模型。基于DS理论进行网络安全威胁信息融合和情景识别，采用概率风险分析进行逐层风险量化和网络安全风险判别，并以低轨道卫星通信网为例进行网络安全风险评估仿真实验，结果验证了该评估模型和方法能有效识别威胁情景，并提高风险评估判别的准确性。

关键词：DS证据理论；协商目标风险分析系统；情景感知；低轨道卫星通信；网络安全；风险评估

Network Security Risk Assessment Model and Method Based on Situation Awareness

QI Yong, WANG Yan, LI Qian-mu
(School of Computer, Nanjing University of Science & Technology, Nanjing 210094, China)

【Abstract】 In view of network security situation awareness framework's lack of a precise mathematical quantitative method to network information security risk assessment, a network risk assessment model based on network security situation awareness framework is proposed by combining DS evidence theory and Consultative Objective Risk Analysis System(CORAS). Network security threats information fusion and situation perception based on DS evidence theory, hierarchical risk quantitative analysis based on probabilistic risk analysis, and risk discrimination. Low earth orbit satellite communication network is taken as an example to make a simulation and assessment. Experimental results show the proposed model and method can effectively identify threat situation, and increase the accuracy of risk assessment discriminant.

【Key words】 DS evidence theory; Consultative Objective Risk Analysis System(CORAS); situation awareness; low earth orbit satellite communication; network security; risk assessment
DOI: 10.3969/j.issn.1000-3428.2013.04.037

1 概述

情景感知(Situation Awareness, SA)[1]概念源于对航天航空领域人为因素的研究。文献[2]定义SA是对一定时间、空间域内元素属性的感知，即对含义的理解和近期状态的预测。文献[3]受空中流量控制(Air Traffic Control, ATC)情景识别概念的启发，在网络安全领域提出情景感知框架NSSA(Network Security Situation Awareness)。网络安全情景指被监控网络的全局安全状态、某个时间窗口遭受的攻击和对网络安全总目标的影响，NSSA描述整个网络的实时风险信息以及全局安全风险态势，是当前网络安全评估领域一个新的研究热点。一些学者对NSSA框架模型进行了研究[4]，如提出多感知器数据融合框架、基于网络数据流(NetFlow)的NSSA框架模型、分布式NSSA框架模型，国防科技大学开展了规模网络安全态势感知技术和评估模型研究。但这些框架研究主要是一些定性分析工作，没有精确的风险量化方法。

综合国内外研究工作，本文提出NSSA框架的概念性模型[5]，模型分为3个阶段：(1)情景识别；(2)情景评估；(3)情景预测。

第(1)个阶段为情景识别，是情景感知的基础，采用成熟技术从海量多源异构数据中识别网络安全情景信息，并转化成可理解的格式(如XML)，为情景评估做准备。

第(2)个阶段为情景评估，是情景感知的核心部分，是

基金项目：国家自然科学基金资助项目(61272419)；中国航天CAST创新基金资助项目(CAST200839)；中国航天CALT创新基金资助项目(CALT201102)

作者简介：威 溟(1970－)，男，教授、博士后、CCF会员，主研方向：信息安全风险评估；王 艳，硕士研究生；李千目，副教授、博士后

收稿日期：2012-07-16 **修回日期**：2012-09-14 **E-mail**：qyong@njust.edu.cn

一个动态、实时理解网络安全情景的过程，通过认知安全事件、确定事件间的关系，生成安全情景图。

第(3)个阶段为情景预测，是根据以往和当前网络安全情景得到网络安全态势，根据实时网络信息判定安全趋势的过程。

2 CORAS 风险分析方法

NSSA 框架的概念性模型如图 1 所示。

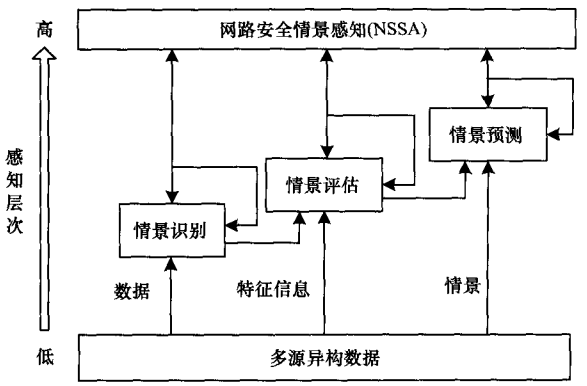

图 1 网络安全情景感知的概念性模型

为弥补 NSSA 框架没有量化的缺点，引入基于 CORAS 框架[6]的风险分析方法，针对情景感知各个阶段进行分析。CORAS 框架是德国、希腊、英国、挪威于 2003 年完成的安全关键系统风险分析平台。

该平台把风险分析技术和基于 UML 的系统建模方法结合起来，包括术语、库、方法论和工具 4 个部分，如图 2 所示。术语定义框架涉及的概念，给出统一化命名标准；方法论给出风险分析的技术、遵循的过程及描述方式，为分析提供理论基础；知识库为风险分析提供先验知识，评估知识库存储每次风险分析的结果数据，提高分析准确率和效率；工具集提供方法的计算工具，并用于实现知识库。

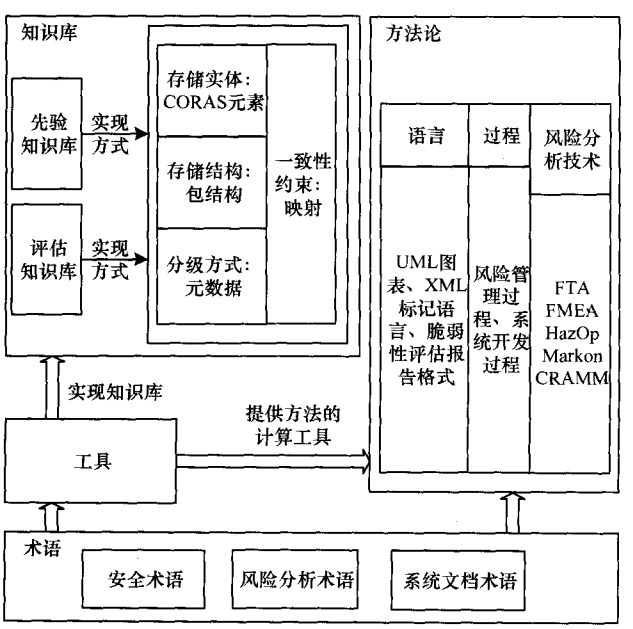

图 2 CORAS 框架的主要组成部分

3 DS 证据理论

DS 证据理论[7]于 1967 年提出，经进一步发展完善，形成了基于信度函数的证据理论。

(1) mass 函数

假设一个决策问题由 n 个可能的决策方向或状态组成一个彼此互斥的全备集合，记为$\{a_1,a_2,\cdots,a_n\}$，将整个集合称为识别框架，记为 Θ。基本概率分配 BPA 函数即 mass 函数是识别框架 Θ 的幂集 2^{Θ} 到[0,1]区间的映射，$m(A)$称为基本概率分配 BPA 或者 m 值，表示证据对 A 的可信度，还可以表述为证据对 A 发生的支持度。一个证据分配给框架 Θ 上的所有子集的 m 值加起来等于 1：

$$\sum_{A\subseteq\Theta} m(A)=1 \tag{1}$$

其中，A 代表框架 Θ 的所有子集，并且 $m(\phi)=0$，即空集合的 m 值为 0。

(2)Dempster 合成规则

Dempster 规则是 DS 理论的基础规则，用于融合 2 个或多个证据。

将识别框架 Θ 上的 s 个独立证据对应的 mass 函数分别记为 $m_1,m_2,\cdots,m_s$，若对于 $\forall A\subseteq\Theta$，经 $m_1,m_2,\cdots,m_s$ 合成后总的 m 值记为 $m(A)$，则 $m_1,m_2,\cdots,m_s$ 的合成规则为：

$$m(A)=m_1(A)\oplus m_2(A)\oplus\cdots\oplus m_s(A)=\begin{cases}0 & A=\phi\\ \dfrac{1}{K}\cdot\sum\limits_{\bigcap_{i=1}^{s}A_i=A}[m_1(A_1)\cdot m_2(A_2)\cdot\cdots\cdot m_s(A_s)] & A\neq\phi\end{cases} \tag{2}$$

其中：

$$K=\sum_{\bigcap_{i=1}^{s}A_i\neq\phi}[m_1(A_1)\cdot m_2(A_2)\cdot\cdots\cdot m_s(A_s)]=1-\sum_{\bigcap_{i=1}^{s}A_i=\phi}[m_1(A_1)\cdot m_2(A_2)\cdot\cdots\cdot m_s(A_s)]$$

证据理论具有如下主要特征：

(1)mass 函数中包含“不确定”的信息，并在 Dempster 合成中保留、融合这些信息得到一个综合结果。

(2)DS 理论不仅能为识别空间中的单个元素分配信任度，还能为它的子集分配信任度。使用 DS 理论融合多个感知器的感知情况，可以有效提高威胁情景识别准确性。

4 网络安全风险评估模型

为了弥补现有 NSSA 框架对网络安全风险评估没有精确量化方法的不足，本文以低轨道(Low Earth Orbit, LEO)卫星通信网为例，引入基于 CORAS 框架的风险分析和概率分析、安全关联树等方法，针对 NSSA 框架各个阶段的特征给出具体的风险分析方法、知识库、术语、实现工具等，提出一种基于情景感知框架的网络安全风险评估模型，如图 3 所示[8]。LEO 卫星通信网由下到上分为安全服务风险、节点风险和通信网风险 3 个风险分析层次。

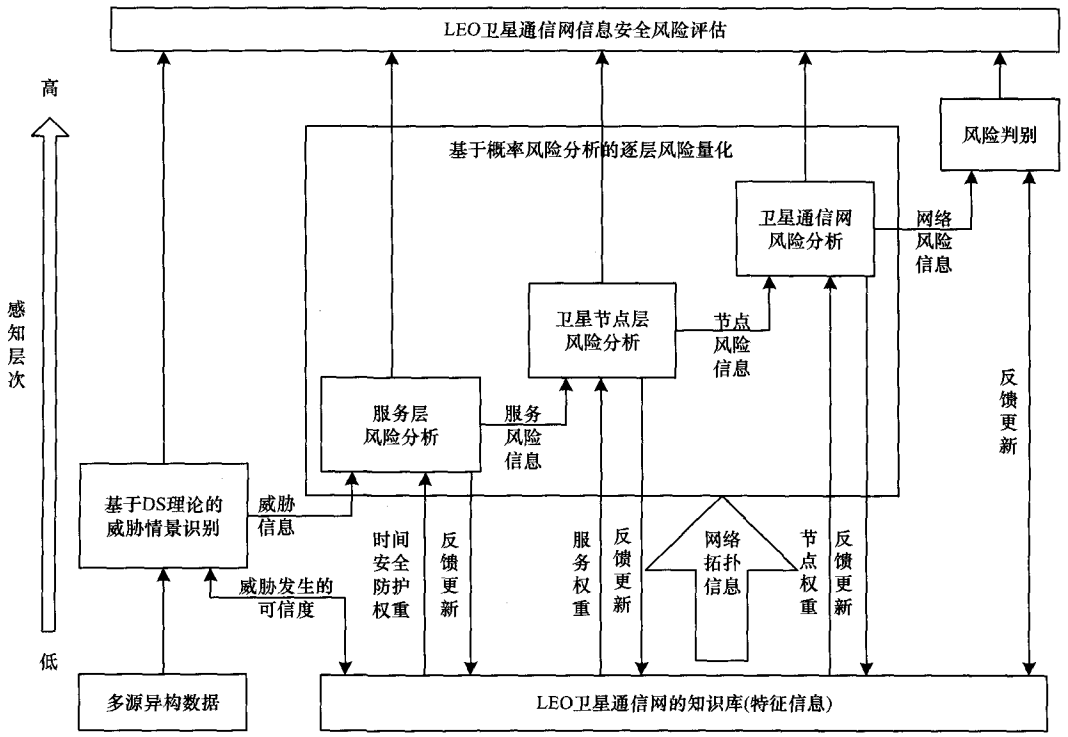

图3 基于情景感知框架的网络安全风险评估模型

模型整个评估分为如下 3 个感知阶段，在每个感知阶段引入反馈更新机制，在评估过程中根据实际情况不断调整更新知识库：

(1)基于 DS 理论的威胁情景识别。采用防火墙、入侵防护系统等网络安全工具作为感知器，感知网络可能存在的攻击信息(包括攻击的类型、可能性等信息)，再基于 DS 证据理论的方法融合各个感知器感知到的攻击信息，得到发生的威胁以及威胁发生的可信度，作为第 2 阶段的输入，从而不需要面对成千上万的警讯数据，提高管理和控制网络的效率。

(2)基于概率风险分析的逐层风险量化。针对第 1 阶段识别的威胁，基于概率分析和安全关联树方法，对服务层风险、卫星节点层风险和网络层风险进行量化分析，并在分析过程中融入时间权重、安全服务在卫星节点上的重要性、卫星节点在网络中的重要性等权重信息以增加评估客观性，同时考虑安全机制的保障作用和风险沿节点关联关系传播的情况。

(3)风险判别。依据第 2 阶段风险分析结果，对整个网络的风险进行判别，包括风险最大的网络节点的判别和网络最容易面临的风险类型的判别。

5 网络安全风险评估方法

5.1 基于 DS 理论的网络威胁情景识别

威胁情景识别的框架为[8]：

(1)术语：威胁、威胁情景、感知器、识别框架、mass 函数、信任度。

(2)方法论：DS 证据理论。

(3)工具：使用防火墙、入侵防护系统、杀毒软件和安全检测技术作为感知器。

(4)知识库：网络扑模型图、感知器感知到各类威胁发生的可信度，如表 1 所示。

表1 各感知器对威胁发生的可信度

可信度		FW	IPS	A-V	SIT
SNMP 威胁	存在	0.4	0.5	0.7	0.7
	不存在	0.6	0.5	0.3	0.3
RPC 威胁	存在	0.4	0.7	0.6	0.6
	不存在	0.6	0.3	0.4	0.4
FTP 威胁	存在	0.5	0.6	0.5	0.6
	不存在	0.5	0.4	0.5	0.4
HTTP 威胁	存在	0.5	0.8	0.5	0.6
	不存在	0.5	0.2	0.5	0.4
TELNET 威胁	存在	0.6	0.7	–	0.8
	不存在	0.4	0.3	–	0.2
DNS 威胁	存在	0.7	0.8	–	0.5
	不存在	0.3	0.2	–	0.5

定义 1 威胁 Threat=(T_name, T_toSA, T_time, T_probability)。其中，T_name 表示威胁名称；T_toSA 表示威胁所影响的安全服务；T_time 表示威胁发生的时间；T_probability 表示威胁发生可能性。

定义 2 按网络应用层程序的类型将威胁 Threat 分为 SNMP Threat、RPC Threat、FTP Threat、HTTP Threat、TELNET Threat 和 DNS Threat。

定义 3 使用防火墙(FireWall, FW)、入侵防护系统

(Intrusion Protection System, IPS)、杀毒软件(Anti-Virus, A-V)和安全检测技术(Security Inspection Technology, SIT)作为感知器从网络多源异构数据中感知可能存在的威胁，识别框架 $\Theta=\{$威胁存在, 威胁不存在$\}$，感知器 $S=\{S_1,S_2,\cdots,S_s\}$，用感知器 S_i 对威胁 $Threat_j$ 的确报率表示感知器 S_i 感知到 $Threat_j$ 存在的可信度 M_{ij}，即 m(威胁存在)=M_{ij}=确报率，用感知器 S_i 对威胁 $Threat_j$ 的误报率表示感知器 S_i 感知到 $Threat_j$ 不存在的可信度 $\tilde{M}_{ij}$，m(威胁不存在)= $\tilde{M}_{ij}$ =误报率，可信度通过实验得到，存储在知识库。每个感知器对某个威胁存在或者不存在的可信度如表 1 所示，表格中未填项表示感知不到相应列的威胁。

基于 DS 理论进行威胁信息融合的示意图如图 4 所示。

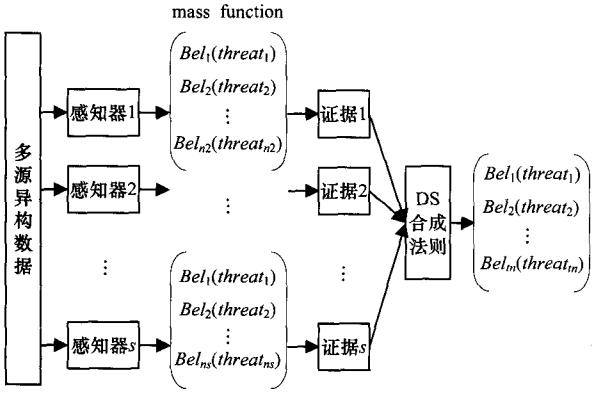

图 4 DS 证据融合示意图

具体步骤如下：

(1)记录感知器感知的一组威胁信息情况。针对威胁 $Threat_j$，感知器 S_i 感知到该威胁存在或不存在情况构成一个证据，记为 m_i，s 个感知器形成 s 个证据，其中识别框架为 $\Theta=\{Threat_j$ 存在, $Threat_j$ 不存在$\}$。如果 S_i 感知到威胁 $Threat_j$，$m_i(Threat_j$ 存在$)=M_{ij}$，简写为 $m_i(Threat_j)=M_{ij}$；$m_i(Threat_j$不存在$)=\overline{M_{ij}}$，简写为 $m_i(\overline{Threat_j})=\overline{M_{ij}}$。如果 S_i 没有感知到威胁 $Threat_j$，则不为 $m_i(Threat_j$ 存在)赋值。各个证据或者分配给 $Threat_j$ 一个基本概率分配值，或者不为其分配，从而得到准确结果。

(2)针对威胁 $Threat_j$，利用证据理论方法融合 s 个证据中关于威胁的信息，感知器感知到的威胁 $Threat_j$ 指单个元素 $Threat_j$，式(2)简化为：

$$m(Threat_j)=m_1(Threat_j)\oplus m_2(Threat_j)\oplus\cdots\oplus m_s(Threat_j)=\frac{1}{K}\cdot[m_1(Threat_j)\cdot m_2(Threat_j)\cdots m_s(Threat_j)] \quad (3)$$

其中：

$$K=\sum_{\substack{s\\ \bigcap_{i=1}A_i\neq\phi}}[m_1(A_1)\cdot m_2(A_2)\cdots m_s(A_s)]=m_1(Threat_j)\cdot m_2(Threat_j)\cdots m_s(Threat_j)+m_1(\overline{Threat_j})\cdot m_2(\overline{Threat_j})\cdots m_s(\overline{Threat_j})$$

得到 $Threat_j\cdot T\_propability=m(Threat_j)$。

(3)按照步骤(2)，得到所有威胁发生的信任度，作为第 2 阶段的输入。

5.2 基于概率风险分析的逐层风险量化

逐层风险量化框架为：

(1)术语：服务风险，直接威胁，间接威胁，访问关联图，访问关联树，节点风险，网络风险。

(2)方法论：概率风险分析，访问关联树。

(3)知识库：时间段的权重 T_1=(0:00~8:00), T_2=(8:00~18:00), T_3=(18:00~24:00)。其中，W_{T1}=0.11；W_{T2}=0.67；W_{T3}=0.22)；安全服务集合 SA；安全服务 SA_j 在节点 N_i 上的相对重要性权值 ws_{ij}；节点 N_i 因为安全服务 SA_j 受到影响而遭受的损失 SA_{ij}_Impact(量化标准 3: 高, 2: 中, 1: 低)；对各安全服务造成危害的威胁，如表 2 所示，V 表示所在列的威胁可能对所在行的安全服务造成危害；安全机制 M_i 对安全服务 SA_j 保障指数 g_{ij}，如表 3 所示(量化标准 3: 高, 2: 中, 1: 低)；N_i 在网络中的相对重要性权值 wn_i 和节点间访问关联图以及访问关联树。

表 2 对各安全服务造成危害的威胁

安全服务	SNMP 威胁	RPC 威胁	FTP 威胁	HTTP 威胁	TELNET 威胁	DNS 威胁
可用性	V	V	V	V	V	V
完整性	V	V			V	
机密性	V	V	V	V	V	
认证	V	V	V		V	
不可抵赖性	V				V	

表 3 安全防护机制对安全服务的保障作用 g_{ij}

防护机制 M_i	安全服务 SA_j				
	可用性 SA_1	完整性 SA_2	机密性 SA_3	认证 SA_4	不可抵赖性 SA_5
加密与密钥管理	2	2	3	1	
访问控制	1	1	1	3	
身份认证			1	3	2
差错控制	3	3			1
无线扩频技术	3	2	2		

整个网络风险[9]由组成网络各节点的风险决定，节点风险与其安全服务遭受的威胁产生的风险有关。在分析得到各个节点安全服务存在威胁情况的基础上，基于概率风险分析(Probabilistic Risk Analysis, PRA)方法，自下而上逐层量化分析相应层的安全风险(包括风险值和发生风险的概率)，最后对整个网络风险进行评估得到总风险。

5.2.1 服务层风险分析

节点 N_i 上服务受到的威胁与 3 个方面有关：(1)直接威胁，即攻击者利用 N_i 的脆弱性攻击的危害。(2)间接威胁，即攻击者在攻击对 N_i 有合法访问关系的 N_k 节点后，利用 N_k 对 N_i 的访问关系访问控制 N_i，对其造成危害。(3)节点本

身安全防护机制对其保障作用。

定义 4 服务风险概率 $PS_{ij}(t)$：N_i 上提供的安全服务 SA_j 在 t 时刻遭受威胁的概率。

定义 5 直接威胁概率 $PS^d_{ij}(t)$：N_i 上提供的安全服务 SA_j 在 t 时刻遭受直接威胁的概率。

$$PS^d_{ij}(t)=1-\prod_{Thr\in Th^t_{ij}}(1-Thr\cdot T\_probablity) \tag{4}$$

定义 6 间接威胁概率 $PS^i_{ij}(t)$：N_i 上提供的安全服务 SA_{ij} 在 t 时刻遭受间接威胁的概率。当一个攻击成功利用相应脆弱点对节点 N_A 造成威胁后，利用节点 N_A 对 N_B 的某种关联关系，进一步对 N_B 进行攻击，造成威胁。将 N_A 到 N_B 的访问关联记为 NTC_{AB}，$NTC_{AB}=(A, B, r, p, Threat)$，$r$ 表示 NTC_{AB} 发生所利用的关联关系，p 表示 NTC_{AB} 发生的概率，$Threat$ 表示 NTC_{AB} 发生后对 B 节点造成的威胁。

定义 7 访问关联图 $GA=(N, E)$，如图 5 所示，灰色顶点为风险节点。N 为顶点集，代表网络节点；E 为有向边集，$e(N_3, N_2)$代表相邻节点 N_3 到 N_2 的节点访问关联 NTC_{AB}，由关联节点指向被关联节点。$e(N_3, N_2).r$ 表示 NTC_{AB} 发生所利用的关联关系；$e(N_3, N_2).p$ 表示 NTC_{AB} 发生的概率。

定义 8 节点 N_i 的访问关联树：根节点是指受访问(受评估)的网络节点 N_i；中间节点是指通过一层或多层来访问根节点的节点，叶子节点是风险源(直接受到威胁的网络节点)。访问关联图图 5 中 N_6 对应的访问关联树，如图 6 所示，N_3、N_4 为风险源，根节点 N_6 是指受评估的节点。

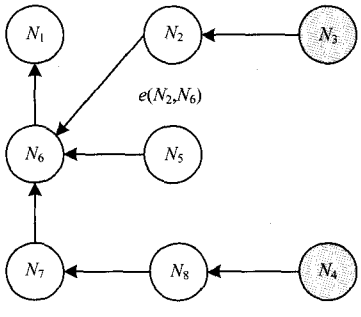

图 5 访问关联图实例

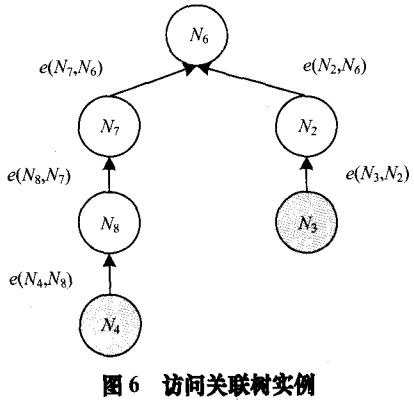

图 6 访问关联树实例

从叶子节点层逐层向上，综合风险源发生威胁的概率 $P_k(t)$、各个关联有向边发生的概率 $e(N_k, N_l).p$，计算得到被评估节点遭受来自风险源传播来威胁概率：

$$P_l(t)=P[\bigcup_{k=1}^{n}N_k\cdot e(N_k,N_l)]=1-\prod_{k=1}^{n}[1-P_k(t)\cdot e(N_k,N_l).p] \tag{5}$$

直到根节点层，结束运算。

$$PS^i_{ij}(t)=1-\prod_{k=1}^{n}[1-P_k(t)\cdot e(N_k,N_i).p] \tag{6}$$

分析得到节点间访问关联图和关联树后，存储在知识库中，并不断更新，得到 $PS_{ij}(t)$：

$$PS_{ij}(t)=1-[1-PS^d{}_{ij}(t)][1-PS^i{}_{ij}(t)] \tag{7}$$

定义 9 安全服务层风险指数 $RS_{ij}(t)$：N_i 上提供的安全服务 SA_j 在 t 时刻所遭受的威胁对其影响程度。

$$RS_{ij}(t)=W_T(t)[PS_{ij}(t)\cdot SA_{ij}\_Impact]\Big/Guard_{ij} \tag{8}$$

其中，$W_T(t\in T_i)=w_{T_i}$；$Guard_{ij}=\max_{k=1}^{mn}g_{kj}$ 表示 N_i 上安全机制对安全服务 SA_j 的保障程度。

5.2.2 节点层风险分析

定义 10 节点风险指数 $RN_i(t)$：节点 N_i 在 t 时刻遭受的威胁对其影响程度。$RN_i(t)$与 N_i 所提供的所有安全服务的安全状况及各个安全服务的相对重要性权值有关，其值愈大，表示风险愈大。

$$RN_i(t)=\sum_{j=1}^{ni}\left[ws_{ij}\cdot RS_{ij}(t)\right] \tag{9}$$

其中，ws_{ij} 表示安全服务 SA_j 在 N_i 提供的所有安全服务中的相对重要性权值。

定义 11 节点风险概率 $PN_i(t)$：节点 N_i 在 t 时刻遭受威胁的概率。$PN_i(t)$为在 t 时刻节点 N_i 上所有安全服务遭受威胁的联合概率。

$$PN_i(t)=1-\prod_{j=1}^{an}[1-PS_{ij}(t)] \tag{10}$$

5.2.3 网络安全风险分析

根据由局部到整体的思想，在得到 t 时刻网络所有节点风险指数 $RN_i(t)$后，就可以确定整个网络的风险指数。

定义 12 网络风险值 $R(t)$：整个 LEO 卫星通信网在 t 时刻总的风险值。$R(t)$与网络中所有节点的信息安全状况及各个节点在网络中的相对重要性权值有关。

$$R(t)=\sum_{i=1}^{n}\left[wn_i\cdot RN_i(t)\right] \tag{11}$$

定义 13 网络风险概率 $P(t)$：整个网络在 t 时刻所有节点遭受威胁的联合概率。

$$P(t)=1-\prod_{i=1}^{n}[1-PN_i(t)] \tag{12}$$

5.3 网络安全风险判别

经过上述方法，可以得到整个网络风险值 $R(t)$、风险发生概率 $P(t)$，各个节点风险值 $RN_i(t)$和风险概率 $PN_i(t)$，以及节点上各个安全服务的风险值 $RS_{ij}(t)$和风险概率 $PS_{ij}(t)$。针对安全服务 $SA_{i,amax}$ 一方面根据对其直接威胁的分析过

程，通过遭受的威胁类型确定节点上存在的脆弱点，针对脆弱性制定相应处理措施；另一方面加强对该安全服务起保障作用的安全防护机制的强度，根据对其间接威胁分析过程中的访问关联树等确定可能的风险源和风险传播路径，针对风险源和风险传播路径，制定相应防护措施。

6 仿真实验

本文以低轨道铱卫星通信网为例，该空间段 N_1~N_4 为卫星节点，N_5 为信关站，N_6 为用户站，N_7 为系统控制站，网络拓扑结构如图 7 所示。A 经信关站 N_5 与 N_6 通信。N_5 与 N_1 建立通信，经 N_2 作为中继路由到 N_4，最后由 N_4 与 N_6 通信，N_7 进行通信控制和管理[8,10]。

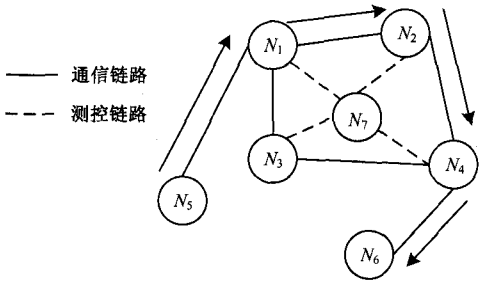

图 7 网络拓扑图

节点 N_i 提供的安全服务 SA_j、服务相对权重 ws_{ij} 以及服务受到破坏后对主机的危害程度 SA_{ij}_Impact 如表 4 所示，服务的相对权重依据节点功能采用层次分析法得到。各节点上运行的安全机制如表 5 所示。

表 4 各节点的安全服务权重和服务受到破坏后对主机的危害

铱卫星 N_1~N_4			地球站 N_5、N_6			系统控制站 N_7		
SA_j	ws_{ij}	SA_{ij}_Impact	SA_j	ws_{ij}	SA_{ij}_Impact	SA_j	ws_{ij}	SA_{ij}_Impact
可用性	0.26	3	可用性	0.24	3	可用性	0.18	2
完整性	0.25	3	完整性	0.23	2	完整性	0.20	2
机密性	0.20	2	机密性	0.16	1	机密性	0.22	3
认证	0.15	1	认证	0.19	2	认证	0.21	3
不可抵赖性	0.14	1	不可抵赖性	0.18	2	不可抵赖性	0.19	2

表 5 各节点的安全机制列表

铱卫星 N_1~N_4	地球站 N_5、N_6	系统控制站 N_7
加密与密钥管理	访问控制	加密与密钥管理
访问控制	身份认证	访问控制
身份认证	差错控制	差错控制
无线扩频技术		

统计 FW、IPS、A-V、SIT 对节点 N_1~N_7 上的威胁感知情况，感知到 N_1、N_5、N_7 存在的威胁，如表 6 所示。以 N_7 为例进行说明，在 t 时刻，感知器 FW、IPS 和 SIP 均感知到 N_7 存在 SNMP、HTTP 和 TELNET 威胁，而感知器 A-V 感知到 N_7 存在 SNMP、HTTP 威胁。其他节点存在的威胁情况同理，V 符号表示存在，空格表示不存在。

表 6 各节点在 t 时刻存在的威胁

可信度	N_7			N_5			N_1		
	SNMP 威胁	HTTP 威胁	TELNET 威胁	RPC 威胁	FTP 威胁	HTTP 威胁	FTP 威胁	TELNET 威胁	DNS 威胁
FW	V	V	V	V	V	V	V	V	V
IPS	V	V	V	V	V	V	V	V	V
A-V	V	V		V	V	V	V		V
SIT	V	V	V	V	V	V	V	V	V

参照感知器感知到各威胁发生的可信度表(知识库)，结合表 6 的信息，基于证据理论融合式(3)得到各个节点发生威胁的信度值(概率)，如表 7 所示。以节点 N_7 为例对概率数据进行说明，N_7 发生 SNMP 威胁、HTTP 威胁、TELNET 威胁的概率分别为 0.784、0.857、0.700，不存在其他 RPC、FTP、DNS 威胁，其他节点同理。

表 7 各节点上发生威胁的概率

威胁	节点 N_7	节点 N_5	节点 N_1
SNMP 威胁	0.784		
RPC 威胁		0.778	
FTP 威胁		0.692	0.692
HTTP 威胁	0.857	0.857	
TELNET 威胁	0.700		0.700
DNS 威胁			0.903

结合表 7 节点 N_7 发生威胁概率和表 2 给出的威胁对各安全服务造成的危害情况，利用式(4)~式(8)得到 N_7 上各安全服务发生威胁的概率和风险值，如表 8 所示。节点 N_7 上的“可用性”安全服务受到直接威胁概率为 0.990 7，不存在间接威胁，故受到的威胁就是 0.990 7，“可用性”安全服务的总风险值为 0.663 798，其他的安全服务同理。

表 8 节点 N_7 上各安全服务的风险

服务	直接威胁概率	间接威胁概率	发生威胁的概率	SA_{7j}_Impact	保障作用 $Guard_{7j}$	总风险值 RS_{7j}
可用性	0.990 7	0	0.990 7	2	2	0.663 798
完整性	0.935 2	0	0.935 2	2	3	0.417 723
机密性	0.990 7	0	0.990 7	3	3	0.663 798
认证	0.990 7	0	0.990 7	3	2	0.995 697
不可抵赖性	0.935 2	0	0.935 2	2	1	1.253 168

同理，得到节点 N_5 和 N_1 的各安全服务风险，如表 9、表 10 所示。

表 9 节点 N_5 上各安全服务的风险

服务	直接威胁概率	间接威胁概率	发生威胁的概率	SA_{5j}_Impact	保障作用 $Guard_{5j}$	总风险值 RS_{5j}
可用性	0.990 2	0	0.990 2	3	2	0.995 183
完整性	0.777 8	0	0.777 8	2	3	0.347 407
机密性	0.990 2	0	0.990 2	1	1	0.663 455
认证	0.931 6	0	0.931 6	2	3	0.416 125
不可抵赖性	0.000 0	0	0.000 0	–	–	0.000 000

表 10 节点 N_1 上各安全服务的风险

服务	直接威胁概率	间接威胁概率	发生威胁的概率	$SA_{1,j}\_Impact$	保障作用 $Guard_{1,j}$	总风险值 $RS_{1,j}$
可用性	0.991	0.952	1.000	3	3	0.670
完整性	0.700	–	0.700	3	2	0.704
机密性	0.908	–	0.908	2	3	0.405
认证	0.908	–	0.908	1	3	0.203
不可抵赖性	0.700	–	0.700	1	2	0.235

利用式(9)、式(10)得到网络节点风险值和风险概率，如表 11 所示。以节点 N_1 为例，N_1 的风险值为 0.494，风险概率为 0.999 999 671 509 755。最后，利用式(11)、式(12)得到整个网络风险值和风险概率，如表 11 所示，整个网络的风险值为 0.302 1，发生风险的概率为 1。

表 11 整个网络的风险值和风险概率

节点	风险 RN_i	风险概率 PN_i
节点 N_1	0.494 0	0.999 999 671 509 775 5
节点 N_5	0.504 0	0.999 998 550 214 400 0
节点 N_7	0.796 3	0.999 999 966 689 520 0
整个网络	0.302 1	1.000 000 000 000 000 0

根据表 11，可知整个网络风险值是 0.302 1，同时：(1)节点 N_7 风险最大，N_5 风险次于 N_7，N_1 风险最小。以节点 N_1 为例，在 N_1 上应该加强对“完整性”和“可用性”2 个安全服务的保护。对于“完整性”来说，一方面需要添加“完整性检测”的安全防护机制，另一方面针对节点上“TELNET”服务的脆弱点修补漏洞；对于“可用性”来说，除了受到直接威胁外，还受到间接威胁，根据访问关联树方法，得到风险源(N_7 的 TELNET、SNMP 威胁和 N_5 的 RPC 威胁)和风险传播路径($e(N_7, N_1)$、$e(N_5, N_1)$)；一方面针对节点 N_1 上“FTP、TELNET 和 DNS”服务的脆弱点修补漏洞，另一方面对 N_7 上“TELNET 和 SNMP”服务和 N_5 上“RPC”服务的脆弱点进行修补。(2)节点 N_1、N_5 和 N_7 的风险概率都很高，N_7 最高，需要重点保护。

7 结束语

本文结合 DS 证据理论和和 CORAS 风险分析等方法，提出一种基于情景感知框架的网络安全风险评估模型，进行威胁情景识别，并基于概率风险分析进行逐层风险量化，引入节点访问关联树，得到节点风险源和传播路径，采用知识库反馈更新机制，增加风险评估判别的准确性。该模型和方法的特点有：(1)依据直接威胁分析得到节点脆弱性，针对性地制定修补漏洞措施；(2)依据各安全服务遭受的威胁，针对性地加强相应安全防护机制；(3)依据间接威胁分析得到风险源和风险路径，制定消减甚至消除风险源和风险传播路径的措施。仿真实验结果验证了评估模型和方法的有效性。

参考文献

[1] Zhang Yong, Tan Xiaobin, Xi Hongsheng. A Novel Approach to Network Security Situation Awareness Based on Multiperspective Analysis[C]//Proc. of International Conference on Computational Intelligence and Security. [S. l.]: IEEE Computer Society, 2007: 768-772.

[2] Kokar M M, Matheus C J, Baclawski K. Ontology-based Situation Awareness[J]. Information Fusion, 2009, 10(1): 83-98.

[3] Bass T. Cyberspace Situational Awareness Demands Mimic Traditional Command Requirements[J]. AFCEA Signal Magazine, 2000, 54(6): 83-84.

[4] Lai Jibao, Wang Huiqiang, Zhu Liang. Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory[C]//Proc. of International Conference on Computational Intelligence and Security. [S. l.]: IEEE Computer Society, 2006: 1545-1548.

[5] 刘效武，王慧强，梁 颖，等. 基于异质多传感器融合的网络安全态势感知模型[J]. 计算机科学，2008，35(8)：69-73.

[6] Vraalsen F, Braber F, Hogganvik I, et al. The CORAS Tool-supported Methodology for UML-based Security Analysis[EB/OL]. (2008-12-04). http://coras.sourceforge.net/documents/CORAS-framework-report.pdf.

[7] Sun Lili, Srivastava R P, Mock T J. An Information Systems Security Risk Assessment Model Under Dempster-Shafer Theory of Belief Functions[J]. Journal of Management Information Systems, 2006, 22(4): 109-142.

[8] 王 艳. LEO 卫星通信网安全风险评估模型与方法[D]. 南京：南京理工大学，2011.

[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(4)：885-897.

[10] 孙利民，卢泽新，吴志美. LEO 卫星网络的路由技术[J]. 计算机学报，2004，27(5)：659-667.

编辑 顾逸斐