分簇结构战术互联网中信任评估模型研究

刘 敏[1], 韩继红[1], 王亚弟[1], 黄 河[2]
(1. 信息工程大学 电子技术学院, 郑州 450004; 2. 中国人民解放军 61938 部队, 北京 100840)

摘 要: 通过对现有典型信任评估方案进行分析比较,提出了分簇战术互联网中基于隶属云理论的信任评估方案,给出了簇内信任和簇间信任的建立、合成与更新公式。方案基于分簇的网络结构,将大量的信任信息限制在簇内,有效减少了实体的存储和控制开销,降低了能量损耗,延长网络生存时间,更加适合于战术互联网环境。

关键词: 信任评估; 簇; 云理论; 信任合成
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2010)07-2661-04
doi:10.3969/j.issn.1001-3695.2010.07.074

Trust evaluation model in cluster-based tactical Internet

LIU Min[1], HAN Ji-hong[1], WANG Ya-di[1], HUANG He[2]
(1. *School of Electronic Technology, Information Engineering University, Zhengzhou* 450004, *China*; 2. *PLA* 61938 *Unit, Beijing* 100840, *China*)

Abstract: Basing on analyzing some typical trust evaluation schemes, this paper presented a cloud theory based trust evaluation scheme in cluster-based tactical Internet and introduced the establishment, composition and updating formula of trust between entities intra and inter cluster. With the use of clustering, restrained most trust information in cluster, thus cuts down the cost of store and control, reduced energy consumption and then prolonged the network duration. The proposed scheme is much more suitable for Tactical Internet environment.

Key words: trust evaluation; cluster; cloud theory; trust composition

战术互联网(TI)是互联的战术无线电台的集合[1],是一种无中心、自组织、多跳的无线网络。战术互联网一般配置在战场前沿,处于敌我混杂的地域,且由于其采用无线信道、有限电源、分布式控制等技术和方式,更容易受到被动攻击、主动入侵、拒绝服务、剥夺“睡眠”、伪造等网络攻击。战术互联网的安全就成为其应用首先应考虑的问题。

安全与信任是紧密联系的。安全可以为信任的创建提供可靠的通信和信息保护,防止信任或证据的暴露;信任是安全的基础,只有被信任的实体才能获得重要信息,同时,信任可以对安全进行增强,尤其是在不稳定的网络环境中。战场环境下,在向其他实体提供某些信息(战场态势、上级命令、友军信息)或与其进行合作之前,实体之间必须建立信任关系,否则,便无法进行安全有效的通信。因此,研究信任对于保证战术互联网的安全具有重要的意义。

1 相关工作

在研究开放网络中安全问题的过程中,一些学者在不同的研究背景下采用不同的方法,基于不同的理论提出了各自的信任评估模型。

Beth 等人[2]引入经验的概念来表述和度量信任关系,并给出由经验推荐而引出的信任度推导和综合计算公式,提出了基于经验和概率统计的信任评估模型。Beth 模型采用精确的概率数值把信任描述为完成一次协作的可能性,等同了信任的随机性和不确定性,忽略了信任本身的模糊性。

George[3]将信任推荐归结为带权有向图上的最短路径问题,提出了基于半环的信任评估。引入观念空间的概念,每个观念包括信任值(评估实体对被评估实体的信赖评估)和信心值(信任值的精确性)两部分。用信任值和信心值来表示信任关系,比单纯采用信任值要准确。但是该模型的信任只基于直觉上的需求,缺乏理论基础,而且信任的产生只基于本地观察也不够完整。

Jøsang[4]引入证据空间和观念空间的概念来描述与度量信任关系,并提供了一套主观逻辑算子用于信任度的推导和综合计算。基于 beta 分布函数描述二值事件后验概率的思想,Jøsang 模型对信任的定义较宽松,同时使用了证据空间中的肯定事件和否定事件对信任关系进行度量。但是 Jøsang 模型同样等同了信任的随机性和主观不确定性,忽略了信任本身的模糊性。

唐文等人[5]考察了主观信任的模糊性,运用模糊集合理论对信任管理问题进行建模。给出了信任类型的定义机制和信任的评价机制,并定义了主体信任关系的形式化表示和推导运算规则。但该模型否定了信任的随机性,把模糊性作为信任的惟一特性,且信任评估机制过于复杂,因素评判矩阵的建立具有很大随意性,缺乏工程可行性。

李德毅等人[6]认为在客观世界普遍存在的不确定性中,随机性和模糊性是两种最重要的形式。将随机性定义为由于事件发生的条件不充分,使得条件与结果之间没有决定性的因

收稿日期: 2009-10-21; **修回日期**: 2009-12-10

作者简介:刘敏,硕士研究生,主要研究方向为计算机网络安全(sadan0415@torn.com);韩继红,教授,博导,主要研究方向为计算机网络安全、信息系统安全;王亚弟,教授,博导,主要研究方向为计算机网络安全、信息系统安全;黄河(1982-),男,主要研究方向为网络安全.

果关系,从而在事件的出现与否上表现出不确定性;将模糊性定义为由于事物概念本身模糊,一个对象是否符合这个概念难以确定而造成边界不清的性质。而其提出的隶属云模型能够把定性概念的模糊性、随机性和不确定性有机地结合起来,实现定性定量之间的转换。本文采用云理论来建模战术互联网中实体之间的信任关系。

2　云的基本概念和数字特征

设 Ω 是一个用精确数值表示的论域(可以是一维、二维或多维),T 是与 Ω 相联系的定性语言值。Ω 中的元素 x 对于 T 所表达的定性概念的隶属度 $C_T(x)$ 是一个具有稳定倾向的随机数,隶属度在论域上的分布称为隶属云[6,7],简称云。$C_T(x)$ 在[0,1]上取值,云是从论域 Ω 到区间[0,1]的映射,即 $x \in \Omega$, $x \to C_T(x)$,序对$(x, C_T(x))$称为云滴。

云的数字特征用期望 *Ex*、熵 *En* 和超熵 *He* 来表征,它们反映了定性概念在整体上的定量特征,如图 1 所示。

期望 Ex(expectation):在论域空间中最能够代表这个定性概念的点,是概念量化的最典型样本点。

熵 En(entropy):代表一个定性概念的可度量粒度,通常熵越大概念越宏观。熵还反映了定性概念的不确定性,表示在论域空间可以被定性概念接受的概率大小,即定性概念的模糊度,代表了定性概念的亦此亦彼性。

超熵 He(hyper entropy):熵的不确定性的度量,反映代表定性概念值的样本出现的随机性,揭示了模糊性和随机性的关联。

可见云模型的三个数字特征值把模糊性与随机性有机集合到一起,构成了定性与定量之间的映射。

3　分簇的网络结构

若每个实体都维护网络中所有实体的信任信息,则需要较大的存储空间,且消耗较多的能量来维护信息。因此,笔者着眼于研究战术条件下的信任问题,提出分簇网络中一种信任评估方案,将大量的信任信息限制在簇内,目的是减少实体的维护开销和存储开销,降低其能量损耗,从而延长整个网络的生存时间。典型的两级簇结构如图 2 所示。

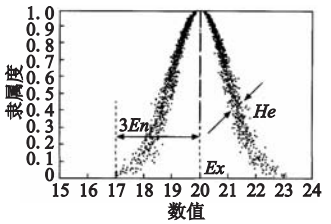

图1　云的数字特征

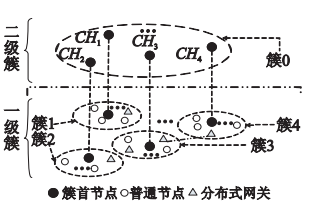

图2　典型两级簇结构示意图

根据一定的簇首选举规则(如最小 ID 算法)将网络分为多个无交叠簇。考虑到战术互联网应用的军事特征:每个作战行动小组一般有一个第一领导者和一个第二领导者。因此,每个簇都选举一个簇首(作为第一领导者)和一个备份簇首(作为第二领导者)。当簇首因失效或离开而无法正常工作时,由备份簇首接管簇首工作,管理本簇。这样,可以减少由于簇首的频繁更替导致的簇重组,增强生成簇的稳定性。

一级簇首选举出后,各簇首可以按照同样的选举规则选举二级簇首,从而形成二级簇(簇首网络),二级簇的簇首又可以形成更高一级簇,依此类推,可以形成多级簇。簇 1、簇 2、簇 3、簇 4 为四个一级簇,其簇首组成二级簇簇 0。

4　簇内信任的建立、合成与更新

簇内信任的建立,遵从图 3 所示的信任评估流程。

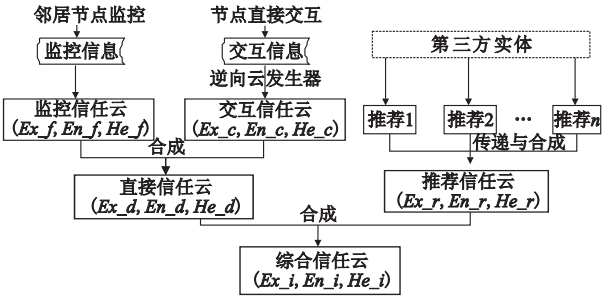

图3　信任评估流程

根据邻居实体的监控信息得到监控信任云,同时,根据实体间的直接交互信任,采用改进的逆向云发生器得到交互信任云,将监控信任云与交互信任云采用一定的规则合成,即得到本实体对被评估实体的直接信任云。在本实体对被评估实体的信任证据不足时,向第三方实体请求推荐信息,将多个第三方实体提供的推荐信任合成得到对被评估实体的推荐信任云。直接信任云与推荐信任云采用合成规则,得到本实体对被评估实体的综合信任云,即代表了本实体在参考其他实体信息后对被评估实体的信任程度。

4.1　直接信任

4.1.1　监控信任

实体处于混杂监听模式,每个簇内实体对本簇内它的所有邻居进行监控,记录监控范围内邻居实体对各种包的处理情况。每条记录包括:报文类型(messageType)、序列号(messageSeq)、目的物理地址(DstMAC)、目的 IP(DstIP)、目的物理地址对应的主机 IP(DstHostIP)、源物理地址(SrcMAC)、源物理地址对应的主机 IP(SrcHostIP)、源 IP(SrcIP)以及报文收集时间(time)。

将记录分类存储处理,对于本实体的邻居实体 i 处的包:

若 $\text{DstIP} \neq \text{DstHostIP}_i$ 且 $\text{DstMAC} = \text{MAC}_i$,则说明此包的终点不是 i 而只是需要其来转发。(In_Forward)

若 $\text{SrcIP} \neq \text{SrcHostIP}_i$ 且 $\text{SrcMAC} = \text{MAC}_i$,则说明此包不是 i 自己产生的而是由它转发的。(Out_Forward)

设定监控周期,计算一个监控周期内实体 i 成功转发包的比率。

每次有一个针对实体 i 的 In_Forward 包,则将其序列号存入线性链表,并将需转发但未转发计数器 needButNot_FW 加 1。此后,若有实体 i 发出的 Out_Forward 包,则在链表中查找是否有其序列号,若有,删除该记录,将 needButNot_FW 减 1,并将成功转发计数器 success_FW 加 1;若没有,则将无须转发却转发计数器 notNeedButDid_FW 加 1。周期结束后,得到本实体监控获得的邻居实体 i 对包的成功转发比率 forward rate 为

$$FR = \frac{\text{success\_FW}}{\text{success\_FW} + \text{needButNot\_FW} + \text{notNeedButDid\_FW}}$$

由于实体总是希望别人为自己转发数据包,可以把数据包的成功转发率作为本实体对转发实体转发行为的满意度,用来衡量实体的监控信任,即对应云模型中的 $Ex_j^i\_f$。而转发满意度完全依赖于包的转发程度,与实体的个人好恶无关,故其不确

定度为0,则监控信任云为$(Ex_j^i_f, En_j^i_f, He_j^i_f) = (FR,0,0)$。

4.1.2　交互信任

将服务满意度分为七个级别,即完全不满意、不满意、稍微不满意、一般、比较满意、满意、非常满意。对应满意度论域$\{l_1, l_2, \cdots, l_7\} = \{0, 0.1, 0.3, 0.5, 0.7, 0.9, 1\}$。评估周期结束后,计算节点间总的交互次数为$N$,每次交互满意度评价为$x_q$,则有$x_q \in \{l_1 l_2, \cdots, l_7\}, (q = 1, 2, \cdots, N)$。

采用改进的逆向云发生器[8]计算直接交互信任云的三个特征值:

a) 根据交互情况计算样本均值$\bar{x} = \frac{1}{N}\sum_{q=1}^{N} x_x$,一阶样本中心矩$d = \frac{1}{N}\sum_{q=1}^{N} |x_q - \bar{x}|$,样本方差$s^2 = \frac{1}{N-1}\sum_{q=1}^{N}(x_q - \bar{x})^2$。

b) $Ex_j^i\_c = \bar{x}$。

c) $En_j^i\_c = \sqrt{\frac{\pi}{2}} \times d$。

d) $He_j^i\_c = \sqrt{s^2 - En^2}$。

则直接交互信任云为$(Ex_j^i_c, En_j^i_c, He_j^i_c)$。

4.1.3　监控信任与交互信任的合成

4.1.1 节用包转发成功率来衡量监控信任,纯粹是用客观的证据来描述信任,没有涉及主观感受;而交互信任是对实体提供服务的满意度,是评估主体的主观感受。因此,两者的合成可以说是客观信任证据与主观信任感受的融合,这样,对直接信任的评价将更加全面。

为减少实体因计算导致的能量消耗,监控信任与交互信任的合成采用简单的线性插值,公式为

$$Ex_j^i\_d = \omega_j^i\_c \times Ex_j^i\_c + \omega_j^i\_f \times Ex_j^i\_f$$

$$En_j^i\_d = \frac{En_j^i\_c(Ex_j^i\_f - Ex_j^i\_d) + En_j^i\_f(Ex_j^i\_d - Ex_j^i\_c)}{Ex_j^i\_f - Ex_j^i\_c}$$

$$He_j^i\_d = \frac{He_j^i\_c(Ex_j^i\_f - Ex_j^i\_d) + He_j^i\_f(Ex_j^i\_d - Ex_j^i\_c)}{Ex_j^i\_f - Ex_j^i\_c}$$

其中:$\omega_j^i\_c$ 和 $\omega_j^i\_f$ 分别为交互信任与监控信任所占的权重,两者和为 1。

得到直接信任云后,存储于直接信任表中,以便用来为其他实体提供推荐信任。

4.2　间接信任

间接信任也称做推荐信任,当两个实体之间的直接信任证据不充分时,就需要其他实体的推荐信任,从而可以更全面地对被评估实体进行信任度量。

实体在提供推荐时,只发送直接信任值,而不包括其根据其他实体的推荐得到的对被评估实体的信任水平,这样可以防止推荐信息形成环路,从而导致自己发出的推荐信息又返回来影响自己的判断。

4.2.1　推荐信任的传递

在请求推荐信息时,有可能经过多个中间实体,如图 4 所示,在$i \sim j$的路径上有$m(m \geqslant 2)$个中间实体$k_1, \cdots, k_m$。其中:k_0即实体i,k_{m+1}即实体j。

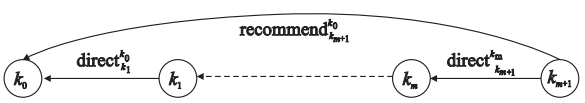

图4　推荐信任的传递

则 i 对 j 的推荐信任为

$$Ex_{k_{x+1}}^{k_x} = \prod_{x=0}^{m} Ex_{k_{x+1}}^{k_x}\_d$$

$$En_{k_{x+1}}^{k_x} = \min\left(\sqrt{\sum_{x=0}^{m}(En_{k_{x+1}}^{k_x}\_d)^2}, 1\right)$$

$$He_{k_{x+1}}^{k_x} = \min\left(\sum_{x=0}^{m} He_{k_{x+1}}^{k_x}\_d, 1\right)$$

特别地,当 $m = 1$ 即中间实体直接向实体 i 推荐 j 的信息时,此传递公式也同样满足。

4.2.2　推荐信任的合成

实体 i 在请求获得推荐信任时,可能有多个推荐者,这就涉及到推荐信任的合成问题,如图 5 所示,n 为推荐者数目。

由于每个推荐者在实体 i 心目中的地位不同,不同的推荐者具有不同的推荐权重,将 i 对各推荐者的信任度标准化后作为相应推荐信任的权重。由于簇首在实体心目中的地位最高,一般具有最大的信任度,在所有推荐者中,簇首具有最大的推荐信任权重,其对综合信任度的影响最大。

推荐实体 k_x 在作为 i 对 j 信任评估时的推荐权重为

$$\omega_{k_x}^i\_r = \frac{Ex_{k_x}^i\_d}{\sum_{x=1}^{n} Ex_{k_x}^i\_d}$$

在对推荐信任进行合成时,需要满足聚合原则,即从多个路径获得的信任的可信度应大于从单个路径获得的信任的可信度,这与人类社会中的交互也是相同的,将许多人对同一个人的观点综合,显然应该比其中某一个人的观点要更客观更全面。采用如下的信任合成式:

$$Ex_j^i\_r = \sum_{x=1}^{n} \omega_{k_x}^i\_r \times Ex_j^{k_x}\_d$$

$$En_j^i\_r = \sqrt{\sum_{x=1}^{n}(\omega_{k_x}^i\_r \times En_j^{k_x}\_d)^2}$$

$$He_j^i\_r = \sum_{x=1}^{n} \omega_{k_x}^i\_r \times He_j^{k_x}\_d$$

4.3　直接信任与间接信任的合成

在进行信任评价时,在获得了第三方的推荐信任后,需要将直接信任与推荐信任进行合成,得到评估实体对被评估实体的综合信任。为了减少实体的计算消耗,同样采用线性插值来合成直接信任与间接信任,公式如下:

$$Ex_j^i\_i = \omega_j^i\_d \times Ex_j^i\_d + \omega_j^i\_r \times Ex_j^i\_r$$

$$En_j^i\_i = \frac{En_j^i\_d(Ex_j^i\_r - Ex_j^i\_i) + En_j^i\_r(Ex_j^i\_i - Ex_j^i\_d)}{Ex_j^i\_r - Ex_j^i\_d}$$

$$He_j^i\_i = \frac{He_j^i\_d(Ex_j^i\_r - Ex_j^i\_i) + He_j^i\_r(Ex_j^i\_i - Ex_j^i\_d)}{Ex_j^i\_r - Ex_j^i\_d}$$

与人类社会关系中人更多地倾向于自己的观点类似,实体综合考虑直接信任与间接信任时,往往更加相信自己的判断,即直接信任的权重往往大于间接信任。

4.4　信任更新

实体间的信任不是一成不变的,而是随着它们之间交互的增多以及了解的深入不断变化,这就需要对信任进行更新。

信任更新有定期更新和事件更新两种。定期更新就是设定评估周期,每到周期结束时,就将以往信任值与本周期形成的信任值合成,得到新的信任值。事件更新主要是根据实体的一些特殊行为调整信任值,若有好的表现,则信任值提高;否则,信任值降低,笔者将在下一步制定策略对其进行调整,这不

是本文的研究内容。

根据社会学观点,信任是对历史经验的总结;而从统计意义上看,信任具有随时间衰减的特性,即相比于久远的信任,近期的信任更具影响性。因此本文引入时间衰减因子来度量信任的时间特性,采用指数函数作为衰减特性函数:$\gamma(t)=e^{\lambda(t-t_0)}$。其中,$t_0$ 为当前时刻,λ 用来调整信任随时间衰减的速度。

采用一个 FIFO 队列来模拟信任随时间衰减的特性,如图 6 所示。

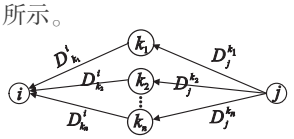

图5 推荐信任的合成

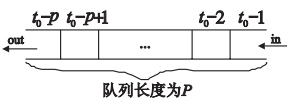

图6 存储历史声誉值的FIFO队列

将本周期产生的综合信任值插入到定长声誉队列队尾,同时所有的信任值向前移动一个位置,而队首的信息被丢弃。队列长度取决于对历史信息的重视程度,对历史信息越重视,队列长度 p 就越大。

则当前时刻的历史信任云为

$$Ex_j^i\_h(t_0)=\sum_{t_x=t_0-p}^{t_0-1}e^{\lambda(t_x-t_0)}\times Ex_j^i\_i(t_x)$$

$$En_j^i\_h(t_0)=\sqrt{\sum_{t_x=t_0-p}^{t_0-1}(e^{\lambda(t_x-t_0)}\times En_j^i\_i(t_x))^2}$$

$$He_j^i\_h(t_0)=\sum_{t_x=t_0-p}^{t_0-1}e^{\lambda(t_x-t_0)}\times He_j^i\_i(t_x)$$

则在考虑了历史信任的影响后,当前时刻实体 i 对 j 的综合信任云$(Ex_j^i_i,En_j^i_i,He_j^i_i)$由本周期产生的综合信任云$(Ex_j^i_i(t_0),En_j^i_i(t_0),He_j^i_i(t_0))$与历史信任云$(Ex_j^i_h(t_0),En_j^i_h(t_0),He_j^i_h(t_0))$采用线性插值得到。

5 簇间信任的建立、合成与更新

不同簇的实体只有作为能够相互通信的分布式网关时才进行相互监控,但分布式网关之间的监控信息不作为证据推荐给其他实体,而只用来建立分布式网关之间的信任关系。

5.1 簇间推荐信任的建立与合成

各级簇之间的关系可以用图 7 所示的树型结构来表示。CH_1 和 CH_2 为二级簇簇首,对应的两个二级簇的簇内成员分别为 $CH_{11}\cdots CH_{1n}$ 和 $CH_{21}\cdots CH_{2m}$,各代表一个一级簇簇首。每个一级簇又由多个普通成员组成,如一级簇簇 A 由 $CM_{111}\cdots CM_{11p}$ 等 p 个普通成员实体组成。

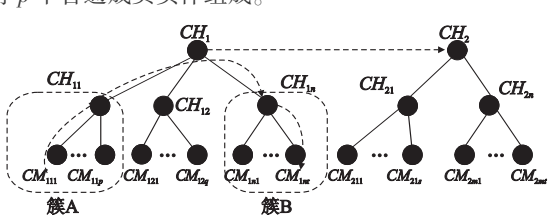

图7 各级簇关系树型图

在建立簇间实体的信任关系时,需要各个簇首的参与,形象地可由树型图中各节点间的有向线来表示。例如,若簇 A 中普通成员 CM_{111} 要建立对簇 B 中普通成员 CM_{1nr} 的信任评估,则沿着有向虚线的方向,由 CM_{111} 对簇首 CH_{11}、簇首 CH_{11} 对簇首 CH_{1n}、簇首 CH_{1n} 对 CM_{1nr} 的综合信任采用信任传递公式复合而成。

假设 i、j 为一级簇内实体,簇首分别为 CH_i、CH_j,两个簇首所在二级簇簇首为 CH。则簇间推荐信任公式如下:

a)实体 i 对二级簇簇首 CH 的推荐信任云

$$Ex_{CH}^i\_r=Ex_{CH_i}^i\_i\times Ex_{CH}^{CH_i}\_i$$

$$En_{CH}^i\_r=\min\left(\sqrt{(En_{CH_i}^i\_i)^2+(En_{CH}^{CH_i}\_i)^2},1\right)$$

$$He_{CH}^i\_r=\min(He_{CH_i}^i\_i\times He_{CH}^{CH_i}\_i,1)$$

其中:$(Ex_{CH_i}^i\_i,En_{CH_i}^i\_i,He_{CH_i}^i\_i)$ 为实体 i 对其簇首 CH_i 的综合信任云,$(Ex_{CH}^{CH_i}\_i,En_{CH}^{CH_i}\_i,He_{CH}^{CH_i}\_i)$ 为一级簇簇首 CH_i 对二级簇簇首 CH 的综合信任云。

b)一级簇首 CH_i 对一级簇首 CH_j 的推荐信任云

$$Ex_{CH_j}^{CH_i}\_r=\sum_{x=1}^{n}(\omega_{CH_x}^{CH_i}\_r\times Ex_{CH_j}^{CH_x}\_d)$$

$$En_{CH_j}^{CH_i}\_r=\sqrt{\sum_{x=1}^{n}(\omega_{CH_x}^{CH_i}\_r\times En_{CH_j}^{CH_x}\_d)^2}$$

$$He_{CH_j}^{CH_i}\_r=\sum_{x=1}^{n}(\omega_{CH_x}^{CH_i}\_r\times He_{CH_j}^{CH_x}\_d)$$

其中:$\omega_{CH_x}^{CH_i}\_r$ 与簇内推荐信任合成中的定义相同,也是对信任值标准化得到的各个推荐信任值的权重。n 为 CH_i 与 CH_j 共同拥有的同等级的邻居实体的数目。

c)二级簇簇首 CH 对普通实体 j 的推荐信任云

$$Ex_j^{CH}\_r=Ex_{CH_j}^{CH}\_i\times Ex_j^{CH_j}\_i$$

$$En_j^{CH}\_r=\min\left(\sqrt{(En_{CH_j}^{CH}\_i)^2+(En_j^{CH_j}\_i)^2},1\right)$$

$$He_j^{CH}\_r=\min(He_{CH_j}^{CH}\_i\times He_j^{CH_j}\_i,1)$$

其中:$(Ex_{CH_j}^{CH}\_i,En_{CH_j}^{CH}\_i,He_{CH_j}^{CH}\_i)$ 为二级簇首 CH 对一级簇首 CH_j 的综合信任云,$(Ex_j^{CH_j}\_i,En_j^{CH_j}\_i,He_j^{CH_j}\_i)$ 为一级簇簇首 CH_j 对实体 j 的综合信任云。

d)其他情况,包括实体 i 对一级簇首 CH_j 的信任、实体 i 对实体 j 的信任、一级簇首 CH_i 对实体 j 的信任等都可由 a)~c)以及簇内建立的信任关系合成。

若簇结构多于两级(图 7 中 CH_1 和 CH_2 与其他同级实体组成更高级簇),则二级簇的不同簇首之间建立信任需要依赖于更高级簇,但基本思想与一级簇簇首建立信任依赖于二级簇是类似的。

5.2 簇间综合信任的计算与更新

直接信任与推荐信任合成为综合信任。公式为

$$Ex_j^i\_i=\omega_j^i\_d\times Ex_j^i\_d+\omega_j^i\_r\times Ex_j^i\_r$$

$$En_j^i\_i=\frac{En_j^i\_d(Ex_j^i\_r-Ex_j^i\_i)+En_j^i\_r(Ex_j^i\_i-Ex_j^i\_d)}{Ex_j^i\_r-Ex_j^i\_d}$$

$$He_j^i\_i=\frac{He_j^i\_d(Ex_j^i\_r-Ex_j^i\_i)+He_j^i\_r(Ex_j^i\_i-Ex_j^i\_d)}{Ex_j^i\_r-Ex_j^i\_d}$$

其中:$\omega_j^i\_d$ 和 $\omega_j^i\_r$ 分别为直接信任与推荐信任所占的权重,两者的和为 1。

除了同属于一个高级簇的各低级簇首之间以及相邻的分布式网关之间有直接信任外,其他簇间实体的信任仅依赖于推荐信任,即只有当 i、j 同为分布式网关或同为低级簇簇首时,直接信任云$(Ex_j^i_d,En_j^i_d,He_j^i_d)$才有意义。其他情况下,$(Ex_j^i_d,En_j^i_d,He_j^i_d)=(0,0,0)$,此时,$\omega_j^i_r=1$。

簇间信任的更新与簇内信任的更新相同,都是考虑到历史信任的影响以及信任随时间的衰减特性,将历史信任与当前信任合成,这里不再作阐述。

(下转第 2667 页)

使有部分攻击取得成功,签名仍然正确,确保所签发数字证书的有效性。

d)存储私钥份额的服务器。采用异构平台,通过操作系统的差异性来提高入侵者攻击的困难,增加 CA 私钥保存的安全性。

3　方案具体实现

为了验证算法的有效性,在 Windows 平台下,基于 Java 和 OpenSSL 对方案进行了实现[7]。Java 中 JCE 提供了处理数据加密、生成消息摘要、进行数字签名、证书管理等功能的类库,可以方便地进行相关开发。但是 Java 无法生成新的证书,本文借助 OpenSSL 来实现生成证书的功能。OpenSSL 是一个开放源代码的软件包,其带有的功能完整的通用加密技术库中包含了完整的加密算法,数字签名算法及证书算法等。其中,OpenSSL 命令行工具提供了一个从操作系统中直接使用 SSL 函数库、Crypto 函数库的方法,也可以直接调用或者修改底层的加密算法程序[8]。使用时下载压缩包后,在 Windows 下编译库函数后得到链接库 ssleay32. dll 和 libeay32. dll 将其加载到 Java 即可。为了方便计算,参数设置:RSA 参数的设置,$p=43$,$q=59$,$e=13$,故 $n=2\ 539$,$d=937$。实际使用时,建议选择 p 和 q 都是 100 bit 的十进制素数,d 就相当于 1 024 bit 二进制数,满足 CA 私钥的实际需求。摘要函数采用 MD5 算法,(t,n)门限秘密,从效率和安全性考虑,取 $t=3$,$n=5$,共享中的重构参数取 $x_i=i$。

具体实现简介如下:Web 服务器采用 Apache 和 Tomcat 技术,Web 页面采用 ASP 技术;采用 MySQL 数据库存放证书信息和密钥信息等;采用基于 HTTPS 的 Web 服务方式为用户提供访问接口,生成证书采用 JDK 中的 Keytool 程序[9]。证书库采用了开放源码的 OpenLDAP 服务器。方法证书生成过程主要如下:生成密钥对文件、生成证书请求、对证书申请签发生成最终的证书。对应这三个过程的主要命令如下:

a)genrsa。用来生成基于 RSA 公钥算法的密钥对文件。

b)req。根据指定密钥文件,并且输入相关的用户信息,来生成用户证书申请文件。

c)ca。自动加入证书颁发机构 CA 的信息,使用指定的私钥对证书进行签名,完成证书的生成。

限于篇幅,具体实现细节不再详细说明。

4　结束语

本文针对 CA 私钥的高安全性需求以及传统算法的不足,提出了一种采用主动秘密共享技术周期性更新 CA 私钥份额,基于 RSA 的分阶段签名算法。该算法的主要优势是在任何时候,都无须重构出 CA 私钥,并且避免了长期攻击可能窃取私钥的安全隐患,提高了 CA 私钥和签名过程的安全性。理论上的分析和实验结果表明,本方案有较高的安全性和一定的应用价值。

参考文献:

[1] 蔡永泉,杜秋玲. 一种 CA 私钥安全管理方案[J]. 电子学报,2005,33(8):1407-1410.

[2] 柴争义,白浩,张浩军. 一种 CA 私钥容侵保护机制[J]. 计算机应用,2008,28(4):910-913

[3] 郭萍. 基于入侵容忍的 CA 认证中心设计[J]. 计算机工程,2007,21(6):70-74.

[4] 柴争义,白浩. 基于主动秘密共享的私钥保护方案[J]. 通信技术,2008,193(1):113-114.

[5] ZHANG Li-wu, FENG Deng-guo. Intrusion tolerant CA scheme with cheaters detection ability[J]. Computer Science, 2005, 37(9): 378-386.

[6] 于佳,郝蓉. 先动的可公开验证服务器辅助秘密 CA 私钥[J]. 北京邮电大学学报,2008,26(10):325-328.

[7] 郭成,李明楚. 主动多秘密 CA 私钥方案[J]. 计算机工程与应用,2009,32(3):107-110.

[8] 张清. 双私钥双随机数认证方案[J]. 计算机研究与发展,2008,45(5):816-822.

[9] 甘元驹,谢仕义. 对安全有效的(t,n)多秘密 CA 私钥认证方案的改进[J]. 电子与信息学报,2007,24(7):81-86.

(上接第 2664 页)

虽然簇间信任的建立需要高级簇的参与,但是在实际应用中,大量的通信都限制在簇内,簇间交互很少,这也就使得簇间实体建立信任关系的频率和可能性较之簇内要低得多,从而仍然保证整个网络有较好的性能。

6　结束语

在对现有开放式网络中典型的几种信任评估方案进行分析的基础上,本文提出了分簇的战术互联网中一种基于隶属云理论的信任评估方案,分别对簇内信任和簇间信任的建立、合成与更新进行了说明。相比于模糊集合理论和概率论理论,隶属云理论能够更好地体现信任的模糊性、随机性及它们之间的关联性,建立的信任模型更加合理。基于分簇结构进行信任评估,将大量信息限制在簇内,相比于平面结构的网络中的信任评估,实体的存储、维护开销都得到了极大的降低。

下一步将着重研究信任基础上的策略调整,即实体如何根据其他实体的一些行为调整自己的策略,如对良好实体给予奖励,对恶意或自私实体给予必要的惩罚等。

参考文献:

[1] IETF. Mobile Ad hoc networks (MANET)[EB/OL]. (2000). http:/www. ietf. org/ html . charters/manet-charter. html.

[2] BETH T. Valuation of trust in open networks[C]//Proc of European Symposium on Research in Security. Brighton: Springer-Verglag, 1999: 59-63.

[3] THEODORAKOPOULOS G. Trust evaluation in Ad hoc networks [C]//Proc of ACM Workshop on Wireless Security. Philadelphia: ACM Press, 2004: 1-10.

[4] JØSANG A. The right type of trust for distributed systems[C]//Proc of New Security Paradigms Workshop. Lake Arrowhead: ACM Press, 1996: 119-131.

[5] 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报, 2003, 14(8):1401-1408.

[6] 李德毅,刘常昱,杜鹢. 不确定性人工智能[J]. 软件学报,2004,15(11):1583-1594.

[7] 李德毅,孟海军,史雪梅. 隶属云和隶属云发生器[J]. 计算机研究和发展,1995,32(6):16-21.

[8] 刘常昱,冯芒,戴晓军,等. 基于云 x 信息的逆向云新算法[J]. 系统仿真学报,2004,16(11):2417-2420.