一种基于信息熵的企业信息系统的安全风险定量评估方法

刘 勇[1] 林 奇[2] 孟 坤[3]

(东北大学 沈阳 110004)[1] (航空工业信息中心 北京 100012)[2] (清华大学计算机系 北京 100084)[3]

摘 要 针对信息系统风险评估中过分依赖主观赋值的现象,提出了基于信息熵的风险评估方法,该方法通过构建威胁-脆弱性矩阵和威胁-损失矩阵,并对所构建的矩阵用信息熵方法分别对其行和列进行处理,从而降低了对主观赋值的依赖性,提高了结果的准确性。最后结合中小企业的实际,设计了一套方便可行的评估流程。利用该方法对典型的企业信息系统进行了实例分析,说明了该方法的有效性。

关键词 信息熵,风险评估,定量方法,企业信息系统

Research on Quantitive Security Risk Assessment Method of an Enterprise Information System Based on Information Entropy

LIU Yong[1] LIN Qi[2] MENG Kun[3]

(Northeastern University, Shenyang 110004, China)[1]

(China Aviation Industry Development Research Center, Beijing 100012, China)[2]

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)[3]

Abstract For the security risk assessment, the result always relies on the value assigned by some queries directly. In order to assess the information system of an enterprise objectively, we proposed an security risk assessment method based on information entropy. By constructing the matrix of Threat-Vulnerability and the matrix of Threat- Loss, we can enhance the result accuracy through dealing with the data of the matrixes by the method of the information entropy. In the end of the paper, we gave an example to explain the efficiency of the proposed method by analyzing an special enterprise information system.

Keywords Information entropy, Security risk assessment, Quantitive method, Enterprise information system

随着计算机技术和网络技术等信息技术的发展与应用,信息安全的内涵在不断延伸,从最初的信息保密性发展到信息的完整性、可用性、可控性、可靠性和不可否认性,进而又发展为"攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)"等多方面的基础理论和实施技术。信息安全风险评估,是指依据国家有关信息安全技术标准,对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学评价的过程[1]。它是保证系统健康运行的关键,为建立信息系统的安全保障体系提供必需的决策依据,因此,在国家战略中,信息系统的信息安全风险评估被给予了充分重视[2]。

1 引言

安全风险评估需要评价信息系统的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响,并根据安全事件发生的可能性和负面影响的程度来识别信息系统的安全风险。风险评估评估方法可分为定性和定量评估两种[3],定性评估方法是指在风险评估过程中,对评估因素的测量使用定性的等级描述等方式实现;而定量评估方法则对评估因素使用测量值进行描述,并利用一定的算法对测量值进行计算而得到安全风险值[4]。采用合理的定量分析方法可以使风险评估结果更具科学性,许多学者在这方面做了大量研究[5,6,11,12]。

已有的许多方法中对于处理收集到的专家数据多数只是经过简单的统计处理,使评估结果过分依赖于专家数据,难以保证结果的准确性。基于此,本文提出一种基于信息风险熵的定量评估方法,使得整个评估在充分利用专家意见的同时,又尽可能地消除主观因素对评估结果的影响。在文章的最后,结合中小企业信息系统的特点,建立了一套方便灵活的适用于中小企业的信息安全风险评估方法。

2 信息系统安全风险评估的要素及计算模型

根据相关的国际、国内标准[1,9],风险评估的要素一般包括资产、威胁、脆弱性、风险和安全措施及它们的相关属性,图1给出了风险要素及其相互间的关系。

风险是整个模型的核心,风险评估的基本要素包括资产、脆弱性和威胁。风险评估围绕其基本要素展开,在对这些要素的评估过程中需要充分考虑业务战略、资产价值、安全事

到稿日期:2009-06-20 返修日期:2009-09-10 本文受国家自然科学基金(60803123)资助。

刘 勇(1973-),男,博士生,主要研究方向为网络管理与网络安全,E-mail:liuy421@tsinghua.edu.cn;林 奇(1969-),男,高级工程师,主要研究方向为信息安全管理与信息系统审计,E-mail:linqi@adr.org.cn;孟 坤(1980-),男,博士生,主要研究方向为网络信息安全等。

件、残余风险等与这些基本要素相关的各类因素。由图1可知业务战略对资产具有依赖性，依赖程度越高，就要求其风险越小；战略对资产的依赖程度越高，则资产的价值就越大；资产价值越大，其面临的风险也会随之增加；而风险的大小除了与资产价值有关外，还受威胁和系统的脆弱性的影响。

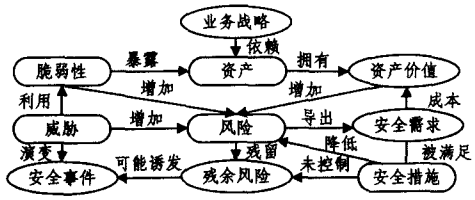

图1 风险要素的关系模型

因此要对信息系统进行风险分析必然要涉及到资产、威胁、脆弱性等基本要素，其基本计算模型为：

$R=f(A,V,T)$

式中，R：风险；A：资产；V：资产的脆弱性；T：威胁。根据各风险要素间的关系，上述模型等价于：

$R=f(I,L(V,T))$

式中，I：资产发生安全事件后对组织业务的影响，即威胁后果；$L()$：威胁利用资产的脆弱性造成安全事件发生的可能性。

因此，要对信息系统进行风险评估，其关键是确定 A,V,T 的值，及它们之间的相互依赖关系。本文采用后一种计算模型，通过采用信息风险熵的方法尽可能地消除主观因素的影响。

3 基于信息熵的风险分析方法

3.1 信息熵[8]

熵是1865年由德国物理学家Glausius作为热力学的一个概念提出来的，1896年，Boftzmann和Planck把熵与系统的可几微观状态数联系起来，说明了熵的统计意义。1948年，Shannon将统计熵概念推广于信息领域，以表示信源的不确定性，其定义如下：

如系统有 n 种不同的状态：$S_1,S_2,\cdots,S_n$，$P(S=S_i)=p_i$ 表示系统处于状态 S_i 的概率，则系统具有不确定性数量 H 为：

$$H=-C\sum_{i=1}^{n}p_i\ln p_i$$

式中，p_i 满足：$0\leqslant p_i\leqslant 1$ 且 $\sum_{i=1}^{n}p_i=1$。

由定义，得到以下命题：

命题1(极值性) 对于系统 S，若其有 n 种不同的状态，且分布率为 $p_1,p_2,\cdots,p_n$，其中 p_i 表示系统处于状态 n 的概率，设该系统的信息熵为 H，则

$$H\leqslant H(\frac{1}{n},\frac{1}{n},\cdots,\frac{1}{n})=C\ln n$$

证明：参见文献[7]。

对于风险评估，由上节的分析，我们知道还需要确定威胁利用脆弱性造成安全事件发生的可能性，对于脆弱性的确定往往采用渗透测试和问卷调查等形式，对于获得的结果往往采用专家赋值的办法来确定对于某种威胁，各种威胁被利用而引起安全事件的可能性。由于单纯地应用这种方法，其结果对专家的主观性依赖性过强，因此，学界和业界在如何增加结果的客观性方面做了大量的研究，给出了一些解决的方法，如德尔菲集体讨论法、模糊分析法[11-13]、故障树分析法[14]、层次分析法等。在文献[5]中，利用熵方法分析了脆弱性的影响，使结果的合理性有了一定的提高。但是由于这些方法本身需要一定的专家赋值，因此这些方法中有关专家赋值的会直接影响结果的准确程度，使得评估结果缺乏一致性。为避免上述结果的发生，我们从分析专家赋值的角度入手，借鉴已有的结论，给出了一种基于信息熵的风险分析方法，通过对专家赋值矩阵作交叉熵方法处理，很大程度上减小了对专家赋值的依赖程度。

3.2 基于信息熵的威胁因素权重计算

对于风险评估中需要评估某个因素(威胁)U，若该要素评判集中指标(系统中存在的脆弱性)为 $r_1,r_2,\cdots,r_m$，通过 n 中方式对各指标进行赋值，可以构造已赋值矩阵：

$$F=\begin{pmatrix}r_{11}&r_{12}&\cdots&r_{1m}\\r_{21}&r_{22}&\cdots&r_{2m}\\\vdots&\vdots&\cdots&\vdots\\r_{n1}&r_{n2}&\cdots&r_{nm}\end{pmatrix}=(r_1\quad r_2\quad\cdots\quad r_m)=\begin{pmatrix}r^1\\r^2\\\vdots\\r^n\end{pmatrix}$$

式中，r_{ij} 表示第 j 种方式对第 i 个指标的赋值，即该方法认为给脆弱性在威胁 U 下可能造成安全事件发生的概率，且满足 $\sum_{j=1}^{m}r_{ij}=1$。

对于上述矩阵，若 r^1 中指标支持度相差较小，则说明该方法收集的数据缺乏说服力，对综合评价的贡献较小；相反，若指标支持度相差较大，说明评定结果分散，该方法收集的数据有一定的针对性，具有较高的说服力，应在综合评价中起关键作用。

根据前面的分析，我们知道信息熵恰好可以很好地反向反映指标支持度的分散程度，因此，用下列熵来度量方法 i 的相对重要性：

$$H_i=-\sum_{j=1}^{m}r_{ij}\ln r_{ij}$$

由命题1可知：$H_i\leqslant\ln m$

对 H_i 做归一化处理：

$$e_i=-\frac{1}{\ln m}\sum_{j=1}^{m}r_{ij}\ln r_{ij}$$

可以得到方法 i 的相对关键程度，且 $0\leqslant e_i\leqslant 1$。$e_i$ 越大，则说明对系统风险评估的贡献越小。

为了使计算值可以正向地反映该方法的重要程度，我们用 $1-e_i$ 表示其重要程度，为了计算方便，对其进行归一化处理，得到：

$$\alpha_i=\frac{1}{n-\sum_{i=1}^{n}e_i}(1-e_i)$$

则 $0\leqslant\alpha_i\leqslant 1$ 且 $\sum\alpha_i=1$。

令 $L=(\alpha_1,\alpha_2,\cdots,\alpha_n)F$，则 L 为因素 U 各影响指标(脆弱性)的赋值。

考虑矩阵 F，向量 r_j 的元素值的差别越大说明其分歧越多，错误判断的机会较多，在评判因素 U 风险时所占的比例应较小，因此可以采用上述类似的方法得到权重系数。

对矩阵 F，令 $r'_{ij}=\frac{r_{ij}}{\sum_{i=1}^{n}r_{ij}}$，通过列规则化，构成新的矩阵 F'；对于 r_i'，用 $H_i'=-\sum_{i=1}^{n}r'_{ij}\ln r'_{ij}$ 表示其重要程度，对其进行归一化，得 $\beta_j=\frac{H'_i}{\sum_{j=1}^{m}H'_j}$。

于是可以得到威胁因素 U 引起的某种安全事件概率赋值为：

$$P_U = L \cdot (\beta_1, \beta_2, \cdots, \beta_m)^T = L = (\alpha_1, \alpha_2, \cdots, \alpha_n) F (\beta_1, \beta_2, \cdots, \beta_m)^T$$

因此，通过进行行和列的信息熵方法的处理，很大程度上不仅避免了对某种特定测试方法的依赖，而且还可以有效地降低误差值。应用该方法，对于不同的威胁因素，可以得到基于评估系统的相应的赋值。

3.3 威胁后果属性及其权值确定

在信息安全评估中，威胁后果的量化是一个重点和难点问题。现实中，某种特定的威胁可能对信息系统造成不同层面的威胁，常见的威胁后果包括“不能进行关键操作”、“损失生产力”、“损失收入”、“损害公共信誉”、“危害公共安全”等。我们为威胁后果设置不同的属性，对于每一种属性都对应着一个权重表示后果引起对该属性的影响程度。这里设属性集合 $ATT=\{a_1, a_2, \cdots, a_k\}$，每个属性的赋值集合为 V，对于某一个后果 E，用 w_i 表示对属性 a_i 的赋值，其中 $w_i \in V$。为确定某个安全事件的后果严重程度，同样可以采用多种方法赋值，采用基于信息熵的方法减少主观影响，从而确定威胁后果的大小，具体方法可以参见 3.4 节。为简便起见，介绍一种简单的统计方法，即构造赋值矩阵。

$$B=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & \cdots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nm} \end{pmatrix} = (b_1 \quad b_2 \quad \cdots \quad b_m) = \begin{pmatrix} b^1 \\ b^2 \\ \vdots \\ b^n \end{pmatrix}$$

式中，b_{ij} 表示用第 i 种方法对属性 j 的权重赋值，$b_{ij} \in V$，则对各属性的赋值可以简单地认为是所有方法的平均值，即 $w_j = \frac{\sum_{i=1}^{n} b_{ij}}{n}$。

下面将确定属性 i 对后果的影响程度 λ_i。对 B 进行规范化处理，构造新矩阵 B'，使得 B' 中的元素 b'_{ij} 满足：$b_{ij}' = \frac{b_{ij}}{\sum_{i=1}^{n} b_{ij}}$。对于矩阵 B' 和列向量 b_i'，确定其信息熵 $H_{b_i}' = -\sum_{i=1}^{n} b'_{ij} \ln b'_{ij}$，归一化得到 $\lambda_i = \frac{H_{bi}'}{\sum_{j=1}^{m} H_{bj}'}$。

从而，可以得到所分析的威胁后果的值 $W=(w_1, w_2, \cdots, w_m) \cdot (\lambda_1, \lambda_2, \cdots, \lambda_m)^T$。

3.4 风险计算方法

由 3.2 节可以得到在系统脆弱性存在的情况下某种安全事件(威胁后果)发生的概率。通过调查、收集历史上发生的有关威胁事件的资料数据，确定需考察的安全事件种类，假设 $C=\{c_1, c_2, \cdots, c_l\}$，那么对于 c_i，分别进行 3.2 节和 3.3 节中的计算，得到该安全事件在威胁 U 存在的条件下发生的概率为 p_{Ui}，威胁后果值为 W_i，则可以得到该威胁对系统造成的安全风险值 $R_U = \sum_{i=1}^{l} p_{Ui} \cdot W_i$，遍历所有的威胁 U，可以得到系统的风险值 $R = \sum_{U} R_U$。若各威胁存在的概率为 P_U，则可得到系统期望风险值 $R = \sum_{U} P_U \cdot R_U$。

3.5 容许风险程度的设定

对于不同的信息系统其安全要求不尽相同，可以通过两种方式来设定系统的风险容忍程度[13-15]：(1)根据实际情况设定风险值，如各威胁引起的风险值不超过某个固定值 b，系统风险值不超过 B，这里一般要求 $B \leqslant b \cdot |U|$，U 为系统的威胁集合，若满足则认为风险是可以接受的；(2)通过改进前后，测定风险值的差值与其测定前风险值的比值 p 的大小，定义风险容忍程度，一般若 $p \leqslant 0.1$，则认为系统的风险是可以接受的。

如果系统满足容许风险程度，则可认为系统是基本安全的，否则需要进一步的整改。

4 基于信息熵的信息安全风险评估在企业信息系统中的应用

在对信息系统进行风险评估时，根据相关的评估标准[1]，结合第 3.4 节中的计算方法，其评估流程如下：

Step 1 评估准备。确定被评估的系统，分析其历史安全记录，调研信息系统的运行现状，确定相应的安全威胁集合、安全事件集合。常见的安全威胁如表 1 所列。

表 1 企业信息系统的主要安全威胁

编号	威胁名称	说明
1	物理环境威胁	断电、静电、灰尘、潮湿、温度、电磁干扰、洪灾、地震等环境问题和自然灾害
2	软硬件故障	设备硬件故障、通讯链路中断、系统本身或软件bug对业务高效稳定运行的影响
3	内部人员误用或失误	不关心、不专注或缺乏专业技能、没遵守规章制度和流程而导致系统故障或被攻击
4	恶意代码和病毒	具有自我复制和传播能力，对信息系统构成破坏的程序代码
5	黑客攻击	利用黑客工具和技术，对系统进行攻击和入侵
6	管理混乱	安全管理不规范或落实不到位等破坏系统正常运行

Step 2 构造计算矩阵。设计报表，选用多中方法获得关于威胁-脆弱性和威胁-资产的数据，根据第 3 节方法构造相应的矩阵。

Step 3 计算矩阵。按第 3 节的方法，计算矩阵得到 p_{Ui}，W_i，R_U 及 R。

Step 4 风险分析。判断是否达到容许风险程度，如果满足，认为系统基本安全，否则，进入 Step 5。

Step 5 根据计算结果的大小有针对性制定预警和防范措施。

5 典型的中小企业信息系统中的应用

5.1 典型的中小企业信息系统

信息系统作为企业信息化建设的一个重要组成部分，通过建立与互联网的连接，设立 Web 服务器等设备，实现了企业与外部的信息交流与共享；通过建立内部网，可以实现办公自动化，大大提升了企业的工作效率。对于中小企业，其典型的结构如图 2 所示。

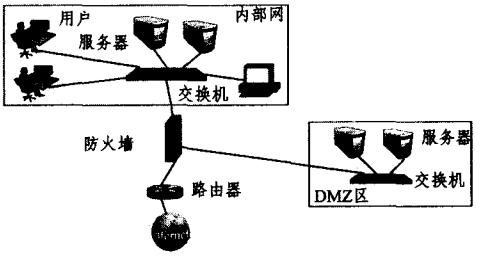

图 2 典型的企业信息系统网络结构

根据标准[1,9,10]，结合上述结构，该信息系统存在的主要威胁应可以按以下方式划分，如表 1 所列。

而对于威胁后果，可以依据标准和安全报告，大致分为系统失效、重要信息被破坏、信息被盗等，其详细情况可以根据被评测系统和相关标准[1]确定。

5.2 基于信息熵的评估方法在中小企业信息系统中的应用实例

针对上述典型的中小企业信息系统，我们以管理混乱为例对该方法加以说明，并通过与传统方法比较说明其合理性。

假设该企业信息系统的脆弱性集合 $V=\{v1:DMZ$ 设置不当；v2：数据无加密措施；v3：无强制访问控制措；v4：员工有不良操作习惯；等$\}$，导致的威胁后果 $D=\{d1:$ 系统失效；d2：信息被窃取；d3：信息被破坏$\}$。

通过采取多种方法，得到关于 d_i 的赋值矩阵分别为：

$$F_{d1}=\begin{pmatrix}0.3 & 0.1 & 0.3 & 0.3\\ 0.25 & 0.25 & 0.25 & 0.25\\ 0.4 & 0.1 & 0.3 & 0.2\\ 0.2 & 0.1 & 0.4 & 0.3\end{pmatrix}$$

$$F_{d2}=\begin{pmatrix}0.2 & 0.6 & 0.1 & 0.1\\ 0.1 & 0.4 & 0.3 & 0.2\\ 0.4 & 0.4 & 0 & 0.2\\ 0.2 & 0.5 & 0.1 & 0.2\end{pmatrix}$$

$$F_{d3}=\begin{pmatrix}0.4 & 0.1 & 0.2 & 0.3\\ 0.25 & 0.25 & 0.25 & 0.25\\ 0.2 & 0.1 & 0.4 & 0.3\\ 0.1 & 0.4 & 0.2 & 0.3\end{pmatrix}$$

如果不知道任何信息，则缺省的赋值方式往往是平均分布，该赋值不能得到专家的任何知识，对评估是没有任何作用的，因此在评估中这样的赋值应较少考虑。下面通过数值计算说明，基于信息熵的评估方法是完全可以消除之中赋值的影响的。利用常规方法，常采用 Dephi 方法，消除影响较小的因素，而后进行计算[5,6]。以 d_1 为例，表现为首先消除 F 的第二行向量，通过计算剩余的数据，可以得到：$L=(0.3\ 0.1\ 0.3\ 0.3)$。

直接采用第 3.4 节中的方法，对于 d_1，不难计算出各方案的权重向量 $\alpha=(0.2541,0,0.3729,0.3729)$，则导致 d_1 发生的脆弱性的权重向量 $L=\alpha\cdot F_{d1}=(0.3\ 0.1\ 0.3\ 0.3)$。与传统方法完全一致，因此，证明了该方法的有效性，并且可以说明该方法简化了计算步骤(不必进行删除行的操作)。

更进一步，根据 3.2 节，通过对 F_{d1} 的列进行信息熵方法的处理，可以得到在管理混乱的情况下，发生安全事件 d_1 的概率为 0.2606。同理可以得到 d2 和 d3 发生的概率分别是：0.1713 和 0.2376。

采取 3.3 节方法，可以得到威胁后果的赋值 w_{di}，这里不妨假设：$w_{d1}=0.8$，$w_{d2}=0.9$；$w_{d3}=0.6$。因此，管理混乱给系统带来的风险值为 0.5052。

采用上述方法可以分别计算出各种威胁对系统的风险值，判断是否满足容许风险程度，若不满足，根据值的大小就可以知道系统面临的最大威胁，再根据脆弱性被利用的概率向量 α 就可以找出影响该威胁的最大影响因素，从而可以给出有针对性的改进措施，改进后再进行新一轮的评估，便形成一个闭环过程；若满足，则给出风险报告，指出系统面临的最大威胁。

该方法的另一个重要应用是指导信息系统的建立，图 3 是某企业信息系统建立过程中通过该方法测定的结果，该系统的风险容许程度采用第一种方法给出，为 $b\leqslant 0.5$。

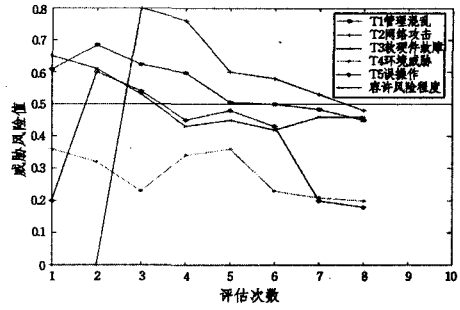

图 3 某企业信息系统建立过程中的信息安全风险评估

从图 3 中可以看出，信息系统刚建立时，由于还不完善，某些威胁还不可能对系统造成威胁后果，因此其风险值为 0，如威胁 T2(外部攻击)随着网络的建立，其风险值急剧增加；而另外一些因素，如 T1，T3 和 T4 更能引起安全事件的发生，其风险值较高，因此相应的改进策略会有针对地加强对这些因素的防范；随着系统化的逐步完善，我们发现所有威胁风险值基本趋于平稳，随着技术和设备的更新，T2，T5 风险值会有较大的减少，但会出现一定的反复，正反应了技术的发展规律；对于 T1，其变化相对较为平稳，说明管理水平的提高是相对缓慢的过程，靠技术弥补管理是不现实的，因此，管理是制约信息系统健康运行的关键因素之一；另外从图中可以看出，在采取一定的改进策略时，某些威胁的风险值会增加，这说明影响系统安全的脆弱性有一定的相关性，与实际情况相符。

总之，通过实例发现，该方法不仅能在简化评估计算中提高准确度，而且还能很好地指导信息系统的建立，从一定角度丰富了风险评估理论。

结束语 现有的信息安全风险评估中，系统数据的获得除少数可以通过相关仪器测量得到以外，大多说还是通过问卷调查等已专家赋值的形式得到，因而，其结果过分依赖于专家赋值，导致结果的随机性大。为减少或避免这种情况的发生，过去的研究往往采用复杂的统计分析、模糊数学等方法对数据进行预处理，大大增加了计算的复杂度。在本文中，通过引入信息熵，大大简化了计算，把数据的预处理集成到风险计算的过程之中，通过实例分析发现，使用该方法得到的评估结果与传统方法得到的结果几乎一致，从而说明了该方法的有效性。但在整个过程中，我们把脆弱性看作是相互独立的，因此，可能会对结果有一定的影响。我们将在今后的工作中，对脆弱性的相关性进行深入的研究，进一步丰富信息安全风险评估理论。

参 考 文 献

[1] GB/T 20984-2007. 信息安全技术信息安全风险评估规范[S]. 中华人民共和国国家标准，2007

[2] 王娜，方滨兴，罗建中，等. “5432 战略”：国家信息安全保障体系框架研究[J]，通信学报，2004，25(7)：1-9

[3] 冯登国，张阳，张玉清. 信息安全风险评估综述[J]. 通信学报，2004，25(7)：10-18

[4] 刘恒，吕述望. 基于模型的安全风险评估方法[J]. 计算机工程，2005，31(9)：129-131

(下转第 56 页)

验中均假定每轮通信中选取的随机检测点数目为4个。

4.2 计算速度与能耗

由于传统的非对称密码体制(如RSA)已被证明不适合无线传感器网络,因此这里只比较IBE和DES之间的计算速度。在DES算法中,采用的是固定56位密钥,以64位为单位对明文进行加解密;在IBE中以64位密钥对相同明文加解密,对比结果见表1。

表1 计算速度对比

	密钥长度(bit)	加密时间(s)	解密时间(s)
DES	56	0.00139	0.00112
IBE	64	4	3.2

从计算速度上来看DES比IBE快了许多,不过考虑到传感器节点的能耗主要在通信工作中(将1bit信息传输100m耗能相当于执行3000条加解密指令[9]),综合看来虽然IBE增加了计算时间,但是总的能耗比起DES并没有大太多,而且作为新型非对称体制的IBE在密钥分配及管理方面比起对称体制的DES具有无可比拟的先天优势[10],所以我们提出的方案具有一定的可实施性。

4.3 存储要求

对无线传感器网络中的节点,理想的内存需求是仅仅存储与相邻节点的密钥。在我们的方法中,每个节点需要保存的信息有在算法中用到的参数π,以及与相邻节点的密钥。与理想的内存开销相比,仅仅多了公共参数π,与所有的存储密钥内存开销相比,这一部分是相对小的。

因此在内存开销方面,我们的方法达到了一定的层次。而对于消息队列的存储,可以根据具体的场景和检测率进行相应的调整,尽量将节点存储的消息限定在一定的范围内,以达到一个最大限度的平衡。

4.4 健壮性

在对称密码体制中,节点之间使用相同的加解密密钥进行通信,因此如果一个节点被俘获,全网就变得不安全,通信无法得到保障[11]。

在我们的算法中,生成的每对对称密钥都不相同,只有进行通信的双方拥有这对密钥。即使交换的公共参数被攻击者获取,他也无法计算出密钥。另外,由于每对节点的密钥不同,当一个节点被破获后,牵涉不到其他节点的安全,更影响不到全网的安全。由此保证了网络的强健壮性。

结束语 本文在前人工作的基础上提出了一种简单有效的选择转发攻击检测方案。通过引入基于超奇异椭圆曲线的IBE算法,并采用无线传感器经典路由协议LEACH中的随机点选取机制,使得网络的安全性得到了很大的提升,理论证明及仿真结果表明我们的方案是可行的。

在未来的工作中,将对本文提出的方案进行更深入的复杂性研究,考虑将累积确认机制(cumulative acknowledge)引入到现有方案,从而解决节点间需要时间同步的问题;与此同时,考虑改进算法,仅利用邻居节点的信息来检测,以达到节省节点能量消耗的目的,从理论和应用角度,得到更优越的结果。

参考文献

[1] 李建中,高宏. 无线传感器网络的研究进展[J]. 计算机研究与发展,2008,45(1):1-15

[2] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures [C]// Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications. 2003:113-127

[3] Yu B, Xiao B. Detecting selective forwarding attacks in wireless sensor networks [C] // Proceedings of the 2nd International Workshop on Security in Systems and Networks (IPDPS2006 Workshop). Greece, 2006

[4] Shamir A. Identity-based cryptography and signature schemes [C]// Advances in Cryptology - CRYPTO'84, Lecture Notes in Computer Science. 1985,196:47-53

[5] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks [C]// Proceedings of the 33rd Hawaii International Conference on System Sciences. 2000

[6] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [C] // Proceedings of Crypto 2001, Lecture Notes in Computer Science. 2001,2139:213-229

[7] Bulusu N, Heidemann J, Estrin D. GPS-less low-cost outdoor localization for very small devices[J]. IEEE Personal Communications, 2000,7(5):28-34

[8] Perrig A, Szewczyk R, Tygar J D, et al. SPINS: security protocols for sensor networks [J]. Wireless Networks, 2002,8(5): 521-534

[9] Wander A S, Gura N, Eberle H, et al. Energy analysis of public-key cryptography for wireless sensor networks [C] // Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications. 2005:324-328

[10] 杨庚,王江涛,程宏兵,等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报,2007,35(1):180-184

[11] 程宏兵,费国臻. 基于身份的无线传感器网络密钥系统[J]. 计算机科学,2007,34(10):116-119

(上接第48页)

[5] 赵冬梅,苏红顺,吴敬. 基于熵理论的无线网络安全模糊风险评估[J]. 计算机应用与软件,2006(8):24-26

[6] 陈鑫,王晓晗,黄河. 基于威胁分析的多属性信息安全风险评估办法研究[J]. 计算机工程与设计,2009,30(1):38-40

[7] 冯瑞,冯步云. 熵[M]. 北京:北京科学出版社,1992

[8] Kapur J N, Kesavan H K. Entropy Optimization Principle with Application[M]. San Diego: Academic Press, 1992

[9] ISO/IES TR 17799[R]. Information Security Management-Code of Practice for Information Security Management. 2000

[10] Risk Management Guide (DRAFT) [S]. National Institute of Standards and Technology. Special Publications 800-30. June 2001

[11] John M G. Fuzzy set computational Processes in risk analysis [J]. IEEE Transactions on Engineering Management, 1991, 38 (2):177-178

[12] Chiclana F, Herrera F, Herrear-Viedma. Integrating Three Representation Models in Fuzzy Multipurpose Decision Making Based on Fuzzy Preference Relations[J]. Fuzzy Sets and Systems, 1998,97:33-48

[13] Feng S, Xu L D. Decision Support for Fuzzy Comprehensive Evaluation of Urban Development[J]. Fuzzy Sets and Systems, 1999,105(1):1-12

[14] Masrhall D A. Coming to Acceptance of ways for Measuring and Ranking Security Properties[C]// First Workshop on Information Security System Rating and Ranking (ACSA). Williamsburg, Virginia, May 2001

[15] Dey P K. Decision Support System for Risk Management: a case study[J]. Management Decision, 2001,39(8):634-649