基于攻击效果的WSN路由安全评估模型

詹永照 饶静宜 王良民
(江苏大学计算机科学与通信工程学院 镇江 212013)

摘 要 为提高无线传感器网络(Wireless Sensor Networks,WSN)的路由安全评估能力,提出了一种基于攻击效果的评估模型。根据路由攻击前后网络安全性能的变化,提出了"网络安全熵"的概念,选取并简化能客观真实地反映安全性的安全评估指标,分析了网络安全熵的计算方法。其次利用Monte Carlo方法进行统计,确定节点的安全度,对安全指标进行归一化处理,通过模型观察攻击效果,评估网络的安全性,并进行安全态势预测,从而提升了WSN网络安全评估的能力,且能够为制定反击敌方的恶意攻击的策略提供依据。经过应用实例的仿真计算与分析,表明该模型能够比较合理地评估网络安全。

关键词 无线传感器网络,路由攻击效果,网络安全熵,Monte Carlo方法
中图法分类号 TP393 **文献标识码** A

Security Evaluation Model of WSN Based on Routing Attack Effect

ZHAN Yong-zhao RAO Jing-yi WANG Liang-min
(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract A security evaluation model based on routing attack effect was introduced to improve the ability of WSN's safety evaluation. Network security entropy was argued to describe the security change after routing attack, we also chose appropriate index and predigested it, to analyze the calculating method of network security entropy. Applying Monte Carlo Method, we got the degree of security, and the security index should be unitary, then we evaluated the security of system and forecasted safe situation by calculating attack effect. Then the ability of WSN's security evaluation could be improved and the model provided basis for better method to resist attacks from enemy. Imitation and analysis of case studies shows that the model is appropriate for security evaluation.

Keywords WSN, Routing attack effect, Network security entropy, Monte Carlo method

1 引言

无线传感器网络(Wireless Sensor Networks,WSN)是由大量体积小、价格便宜、具有无线通信和监测能力的传感器节点组成的[1],在军事、商业、环境监测等众多领域有着广阔的应用前景。与传统无线网络相比,WSN具有体积小、耗能较低等特点。目前在研究WSN时,考虑的关键问题是低能耗和低成本。然而,由于传感节点大多部署在无人照看或者敌方区域,传感器网络安全问题尤为突出。路由和数据转发是无线传感器网络通信的重要部分。因此,建立有效的WSN路由安全评估模型,提高路由安全性,有效控制风险,将成为研究的新热点。基于WSN的路由攻击效果进行路由安全性评估,具有重要的意义。一方面,有效的网络攻击评估准则和检测方法,可以促进WSN网络生存能力的提升,从而提高系统应对复杂环境下各种攻击的能力。另一方面,在应对来自敌方的恶意攻击时,路由攻击效果评估技术可以为网络反击提供合适的应对策略[2]。

关于WSN的安全评估,国内外目前还未形成形式化的定量评估理论和方法,但存在着一些评估模型。现有的安全评估模型可以大致分为以下几类:基于漏洞检测技术的安全评估模型[3,4],用漏洞扫描方法找出目标网络的漏洞信息并进行分析评估,其中Krontiris Ioannis等人提出了一种轻量级的检测WSN中选择转发攻击的方法:节点监视其邻居节点,并与最近的邻居节点合作,使网络恢复正常的运行状态。评估结果虽然较全面,但缺乏整体性,且占用大量时间。文献[5]提出了一个信息系统的综合风险评估模型,它应用层次分析法和模糊逻辑法相结合的方法分析各个风险因素的风险值,评价系统中哪些风险因素值得关注,从而采取相应措施进行控制。该模型可以减少系统的工作量,适用于一些难于完全定量分析的问题。基于人工智能网络的安全评估模型[6],利用网络的学习能力,进行多目标并行评估,可以有效避免主观因素干扰,但需要大量的已知训练样本。

到稿日期:2009-09-15 返修日期:2009-12-01 本文受国家自然科学基金(60703115),中国博士后科学基金特别资助项目(200801357),国家社科基金(09CTJ006),中国博士后科学基金面上项目(20070420955),江苏省青蓝工程优秀青年骨干教师项目,江苏省自然科学基金(BK2007560),江苏省博士后科研资助计划项目(0702003B),江苏大学高级人才科研启动(07JDG080)资助。

詹永照(1962—),男,教授,博士生导师,CCF高级会员,主要研究方向为人机交互与新型网络技术,E-mail:yzzhan@ujs.edu.cn;**饶静宜**(1986—),女,硕士生,主要研究方向为无线传感器网络安全评估;**王良民**(1977—),男,博士后,副教授,主要研究方向为无线传感器网络与信息安全。

本文针对上述问题，提出一种基于安全熵的 WSN 路由安全评估模型，选取能客观真实地反映安全性的安全性能指标，模拟路由攻击，通过安全熵分析攻击效果的计算方法，从而对路由协议的安全性进行评估。

2 路由攻击描述

无线传感器网络的路由协议容易受到各种攻击。敌人能够捕获节点对网络路由协议进行攻击，如路由信息伪造、选择性转发等。受到这些攻击的网络，一方面无法正确、可靠地将信息及时传递到目的节点；另一方面消耗大量的节点能量，缩短网络寿命。由于路由协议受到攻击之后，网络的安全性能失效或者降低，因此可以选取某些安全指标考察受到攻击前后的差值作为路由安全的评价标准。

2.1 常见路由攻击

针对 WSN 的路由攻击很多，常见的可以概括为以下 6 种[7]：(1) 伪造路由信息。攻击者通过假冒、篡改或重放路由信息生成虚假的错误信息，达到分割网络、误导流量、引起阻塞、增加延时的目的。(2) 选择转发攻击。恶意节点通过拒绝转发某些消息，使它们不能被进一步传播。(3) 陷洞(Sinkholes)攻击。通过使泄密节点在路由算法上对周围节点具有特别吸引力，引诱该区域的数据通过泄密节点。(4) 女巫(Sybil)攻击。攻击节点呈现多重身份，使之被其他节点选作下一跳目标的概率更高。(5) 虫洞(Wormholes) 攻击。攻击者通过低延时链路，将某个网络分区中的消息发往网络另一个分区重放。(6) 洪泛(Helloflood)攻击。攻击者利用大功率发射器广播发送 Hello 报文，使得网络的每个节点都误认为攻击者是其邻节点。

几种主要类型的 WSN 路由协议易遭受的攻击，如表 1 所列。

表 1 主要路由协议及易遭受的攻击

路由协议	容易遭受的攻击
基于地理位置的协议 (Geographic Routing)	伪造路由信息，选择性转发，女巫攻击
层次式路由协议 (Clustering Based Protocols)	伪造路由信息，陷洞攻击
定向扩散 (Directed Diffusion)	伪造路由信息，选择性转发，女巫攻击，虫洞攻击，Hello 洪泛攻击
传闻路由 (Rumor Routing)	伪造路由信息，选择性转发，女巫攻击，虫洞攻击

2.2 路由攻击效果的描述

对于一个安全因素 x_i，可以用其安全度 $P(x_i)(0\leqslant P(x_i)\leqslant 1)$来表示其完成安全功能的能力。而安全度的大小又可以从熵的角度来分析，它必然有一个与安全度相对应的安全熵来表示该安全因素的不确定度、混乱度和无序度。当安全度越大，其本身的不确定度、混乱度和无序度就越小；反之，其本身的不确定度、混乱度和无序度也就越大。而攻击前后 WSN 的安全性差值可以作为攻击效果的一个评价标准。由于进行攻击效果评估时只考虑系统遭受攻击前后安全性能的变化，借鉴信息论中“信息熵”的概念，提出了“网络安全熵”的概念，以便很好地描述安全性能的变化。从熵的本质含义出发，熵是一种系统的状态概率 p 的量度 S，即 $S=k\ln p$，其中 k 为常参数值待定系数。在本文计算时，取 $k=1$。“网络安全熵”是对信息安全性的一种描述，熵值越小，表明该网络的安全性越好。对于 WSN 的某一项安全指标 x_i 而言，其熵值可以定义为

$$S(x_i)=-\log_2 P(x_i) \tag{1}$$

从式(1)中可以看出，当安全度 $P(x_i)$越大时，对应的安全熵 $S(x_i)$就越小。显然，WSN 网络受到攻击之后，安全性下降，熵值应该增加。因此，可采用“熵差”

$$\Delta S=-\log_2(P(x_i)'/P(x_i)) \tag{2}$$

来描述攻击效果。其中，$P(x_i)$为网络受攻击前的安全度，$P(x_i)'$为网络受攻击后的安全度。可知，攻击效果越严重，ΔS 越大，反之 ΔS 越小。

3 安全评估模型的建立

3.1 评估指标的选取

随着 WSN 技术的发展与应用，其信息安全的内涵在不断延伸。目前信息的安全通常对应多种性能指标。如何确定能客观真实地反映安全性的指标来评价路由攻击的效果，是关键问题。好的度量应该具有以下特点[8]：(1)一致的度量，没有主观的标准；(2)易于采集，更适合主动获取的方式；(3)以数值或者百分比的形式出现，不是以“高”、“中”、“低”之类的标签来定性；(4)最少使用一个度量单元来表达。根据上述特点，本文结合 WSN 自身的特点，采用系统化分析方法，将安全性度量分为协议层、攻击效果层和安全指标层，其关系是逐步细化的，如图 1 所示。

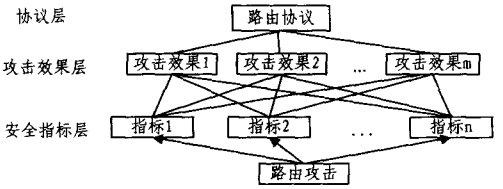

图 1 安全度量层次

图 1 描述了模型的安全度量层次。首先通过路由攻击，测量安全指标层的指标，安全指标层可以通过测量获得的直接数据、主要的安全指标及其所获得的数据来表示，如表 2 所列。其次安全指标层根据对攻击效果层所占的权重，计算各攻击效果的网络安全熵差。攻击效果层主要包含服务质量参数、数据安全性和传输节点的安全性等路由安全的重要方面。最后，再根据攻击效果的熵差及各攻击效果针对路由协议的权重，来计算路由安全熵差。通过本文所提出的反映网络数据传输过程安全性的统计量化方法，对 WSN 的路由安全性进行综合评估。不同的路由攻击对安全指标层的各指标产生不同的影响，可通过测试攻击产生的后果来加权计算攻击效果。

表 2 可测的安全指标及其评测结果的表示

用于评估的主要安全指标	评测结果的量化表示
信道总吞吐率	单位时间内网络各节点之间成功传送的数据量
信道利用率	信道传输有效速率与信道总吞吐率之比
网络传输总延迟	网络所传送的各个报文或分组产生最大的延时
重要节点传输延迟	网络重要节点间传送的各个分组产生最大的延时
网络带宽	网络传送数据的能力
延迟	报文进入网络/节点/链路到离开网络/节点/链路的时间
延迟抖动	平均延迟变化的时间量
响应时间	网络服务请求和响应请求之间的时间
每节点路由表更换周期	每一定时间播发一次(与路由协议有关)

表2给出了安全指标层的可测指标及其结果的表示，在实际评估的过程中，应根据具体路由协议、确定指标的重要性大小，对较繁杂的指标进行筛选[3]。

3.2 节点安全度的确定

构造概率模型，将与WSN路由协议的攻击效果相关的安全性评估指标统一归一化为数据流的过程。根据Monte Carlo方法建立过程模型，再根据安全指标的层次，计算指标的加权熵，从而根据熵值的变化，对路由协议的安全性进行评估。

所谓Monte Carlo方法，就是根据待求随机问题本身的变化和统计规律，构造出一个合适的概率模型或者随机过程，依照该模型进行大量的统计实验，即通过一系列的随机数来模拟这个过程，然后通过对模型或过程的观察或抽样实验来计算所求参数，最后给出所求解的近似值[9]。其分析本质上为一个复杂的概率计算，可以用于模拟攻击，对安全指标进行归一化，进行安全性评估。

路由攻击下的网络安全性是一个复杂的变化过程，因此可以将所有与安全性相关的指标抽象为数据流，建立过程模型。每一个指标用一个进程模拟：一种失效率对应一个{0,1}伪随机数，分别代表正常和失效两种状态。概率模型基于模拟攻击的时间过程。

将一次模拟作为一次随机试验，对网络进行仿真攻击。假设进行 s 次试验，各次试验中指标 x_i 在正常范围内的节点个数分别是 $X_1, X_2, \cdots X_s$，则 $X_1, X_2, \cdots X_s$ 独立同分布。引入随机函数

$$f(Z)=\begin{cases}0, & z\geqslant\beta\\ 1, & z<\beta\end{cases} \tag{3}$$

式中，β 为自定义的、能接受的单项指标正常的最小节点数目，即指标 x_i 正常所满足的临界条件。

根据Monte Carlo方法原理，指标 x_i 正常的概率，即安全度为

$$P(x_i)\approx\frac{1}{s}\sum_{j=1}^{s}f(X_j) \tag{4}$$

式中，j 是指发生的第 j 次攻击试验。

3.3 相关权值的确定

由3.1节的安全度量层次结构可知，根据“熵”的含义，当路由的安全性同时由多个指标 $x_1, x_2, \cdots x_n$ 确定时，以网络安全熵为指标的加权和如式(5)所示

$$S(x)=\sum_{i=1}^{n}\omega_i\times S(x_i) \tag{5}$$

攻击发生前后的安全熵差为

$$\Delta S(x)=\sum_{i=1}^{n}\omega_i\times\Delta S(x_i) \tag{6}$$

式中，ω_i 是指标 x_i 相对于上一层次的权重，n 为衡量某一方面性能的指标的个数。如何准确地设定单个指标的权重，从而计算整个路由协议的网络安全熵是一个重点。在实际应用中，将AHP法应用于安全性评估，确定各层次中各因素的权重。首先，以攻击效果层的要素为准则，对指标的重要性进行排序，去除不重要的指标，并选取重要性常数，得到简化的指标体系。其次，攻击效果层的要素以协议层为准则，进行两两比较，根据评定尺度确定其重要度，建立如下判断矩阵

$$(b_{ij})_{n\times n}=\begin{bmatrix}b_{11} & b_{12} & \cdots & b_{1n}\\ b_{21} & b_{22} & \cdots & b_{2n}\\ & \cdots & & \\ b_{n1} & b_{n2} & \cdots & b_{nn}\end{bmatrix} \tag{7}$$

式中，b_{ij} 表示从判断准则 A 角度考虑要素 B_i 对要素 B_j 的重要程度。其中判断的尺度的取值按相对重要程度取1～9之间的自然数。

根据攻击效果层的判断矩阵，利用方根法计算各元素的相对权重。先求出特征向量 M，对 M 进行归一化处理，得到排序权向量 W，计算矩阵的最大特征根 λ_{max}，再进行一致性检验。一致性指标为

$$C.I.=\frac{\lambda_{max}-n}{n-1} \tag{8}$$

当 $C.I.<0.1$ 时，表明矩阵一致性成立，各项权重无逻辑错误。对第三层次的要素，采用递推的方法得出各层相对于上一层的组合权重向量和平均随机一致性指标。当最底层指标相对于评价总目标的平均随机一致性指标不超过0.1时，认为系统评价的阶梯层次结构模型在各层水平上具有满意的一致性。计算的最终结果便是相对于总目标各评价指标的权重。

4 应用实例与分析

不妨以定向扩散路由协议为例来观察攻击效果。由表1知，定向扩散路由协议易遭受多种攻击。选取选择性转发攻击、虫洞攻击和Hello洪泛攻击，在时间 t 内各进行 s 次模拟。最后计算随着攻击频率的增加，选取网络的几个主要可测指标在正常范围内的概率，通过计算熵差，来观察服务质量、数据安全性和传输节点安全性等攻击效果。最终计算攻击发生时路由的整体安全熵差，从而反映出路由协议的安全性。

4.1 攻击模拟

令 $A=\{a_1, a_2, a_3\}$，其中 a_1=选择性转发攻击，a_2=虫洞攻击，a_3=Hello洪泛攻击。令 $X=\{x_1, x_2, x_3\}$，其中 x_1=吞吐量，x_2=带宽，x_3=信道利用率。在 t=100s的时间内，每种攻击分别发生 $10n$ 次，其中 $n=1,2,\cdots,10$。建立 $A\rightarrow X$ 的映射。令 $Y=\{y_1, y_2, y_3\}$，其中 y_1=服务质量参数，y_2=数据安全性，y_3=传输节点的安全性。建立 $X\rightarrow Y$ 的映射。令 Z=路由安全性，建立 $Y\rightarrow Z$ 的映射。用Monte Carlo方法对每次测量 x_1, x_2, x_3 的值进行统计计算。给定 x_1, x_2, x_3 可接受的正常值 x_1', x_2', x_3'，则 $f(X_i)=\begin{cases}0, & x_i\geqslant x_i'\\ 1, & x_i<x_i'\end{cases}$，$i=1,2,3$，$P(x_i)\approx\frac{1}{10n}\sum_{j=1}^{10n}f(X_j)$，$i=1,2,3$，$n=1,2,\cdots,10$。

代入式(6)中计算攻击前后的熵差 ΔS。若 ΔS 越大，说明攻击效果越显著，从而对路由协议的破坏越严重。反之，若 ΔS 越小，说明攻击效果越不显著，从而对路由协议的破坏越不严重。

4.2 权值计算

构造判断矩阵，指标 (x_1, x_2, x_3) 以上一层 (y_1, y_2, y_3) 为依据的判断矩阵分别是

$$B_1=\begin{bmatrix}1 & 1/3 & 1/8\\ 3 & 1 & 1/3\\ 8 & 3 & 1\end{bmatrix}$$

$$B_2=\begin{bmatrix}1 & 3 & 1/5\\ 1/3 & 1 & 1/9\\ 5 & 9 & 1\end{bmatrix}$$

$$B_3=\begin{bmatrix}1 & 2 & 5\\ 1/2 & 1 & 2\\ 1/5 & 1/2 & 1\end{bmatrix}$$

然后计算第二层次的相对权重。首先求出特征向量 $M_1=(0.246,0.710,2.047)^T$，$M_2=(0.544,0.215,2.293)^T$，$M_3=(1.791,0.831,0.386)^T$。对 M_1,M_2,M_3 进行归一化，得 $W_1=(0.082,0.236,0.682)^T$，$W_2=(0.180,0.072,0.748)^T$，$W_3=(0.595,0.277,0.128)^T$。再计算 $\lambda_{max1}=3.002$，$\lambda_{max2}=3.029$，$\lambda_{max3}=3.006$。一致性指标 $C.I._1=0.001<0.1$，$C.I._2=0.015<0.1$，$C.I._3=0.015<0.1$。表明上述判断矩阵一致性均能成立。W_1,W_2,W_3 中的元素即为各指标相对于上一层的权值。

攻击效果(y_1,y_2,y_3)以上一层 Z 为依据的判断矩阵是

$$A=\begin{bmatrix}1 & 2 & 6\\ 1/2 & 1 & 4\\ 1/6 & 1/4 & 1\end{bmatrix}$$

由 AHP 法计算得特征向量 $M=(1.769,0.974,0.268)^T$，对 M 进行归一化，得 $W=(0.587,0.324,0.089)^T$。再计算 $\lambda_{max}=3.029$，一致性指标 $C.I.=0.0045<0.1$，表明判断矩阵一致性成立。W 中的元素即为各攻击效果的权值。

4.3 熵差计算与分析

进行不同频率的路由攻击时，对系统受攻击后的指标进行测量，将结果代入式(6)，进行熵差计算。计算结果如表 3 所列。其中 f 表示攻击频率(次/100s)，$A=\{a_1,a_2,a_3\}$ 表示攻击的类型，ΔS 表示受攻击后与受攻击前的路由安全熵差，由各层指标加权计算而得。

表 3　受到不同频率路由攻击时的熵差变化

ΔS \ f / a	10	20	30	40	50	60	70	80	90	100
a_1	0.0740	0.2345	0.4150	0.6439	0.8625	1.0291	1.3219	1.7370	2.1520	3.0589
a_2	0.0291	0.2176	0.3959	0.6215	0.8890	1.0000	1.2863	1.6891	2.1203	2.7370
a_3	0.1203	0.2863	0.4639	0.7131	0.9434	1.1520	1.3959	1.8110	2.4739	3.3219

通过计算，表 3 给出了受到不同频率的路由攻击时的安全熵差的变化。从表中可以看出，遭受每一种攻击时，熵差 ΔS 都随着攻击频率的增加而增加。由 2.2 节可知，熵差越大，说明网络受到路由攻击之后对路由造成的安全危害越大。因此，计算结果表明，随着攻击频率的增加，系统的安全性降低。使用熵差 ΔS 可以客观真实地反映 WSN 的路由协议在遭受攻击时的安全性。根据计算结果，可以将路由的安全性分为以下 3 个等级：当 $0\leqslant\Delta S<0.5$ 时，系统为较安全系统；当 $0.5\leqslant\Delta S<1.8$ 时，系统为一般安全系统；当 $\Delta S\geqslant1.8$ 时，系统为不安全系统。

本文针对无线传感器网络路由协议的具体情形，首先以路由的安全性为总体依据，建立安全度量层次，并采用层次分析法确立评估的具体指标。通过比较各个指标的重要性，确定其权值。在此基础上针对不同路由协议给出不同的主要评估指标，从而减少了指标确定的主观因素。其次，利用 Monte Carlo 概率统计的方法对安全度进行归一化，通过多次测量进一步提高了结果的准确性，而且可以避免重复的漏洞检测工作，节省了大量时间和空间，并能够通过概率变化预测系统的安全态势。利用“网络安全熵”的概念计算路由的整体安全水平，计算结果对安全性进行了精确的定量描述，并区分了路由安全等级。利用“熵”的概念，进一步减少了其他因素的干扰，且避免了大量的样本空间。

结束语　本文提出并验证了基于攻击效果的 WSN 路由安全评估模型。结合统计概率和相关权值分析，提出了“网络安全熵”的概念，从而使得模型能够对无线传感器网络的安全性进行客观真实的量化评价，有助于提高无线传感器网络的安全性，从而提高系统应对各种攻击的能力，并能对发现、反击敌方的恶意攻击起到指导作用。实验结果表明，本模型安全评价合理，有较高的应用价值。

参 考 文 献

[1] 裴庆祺，沈玉龙，马建峰. 无线传感器网络安全技术综述[J]. 通信学报，2007，28(8)：113-122

[2] Zhang Y R，Xian M，Wang G Y. A quantitative evaluation technique of attack effect of computer network based on network entropy[J]. Journal on Communications，2004，25(11)：158-165

[3] 肖道举，杨素娟，周开锋，等. 网络安全评估模型研究[J]. 华中科技大学学报，2002，30(4)：37-39

[4] Krontiris I，Dimitriou T，Freiling F C. Towards intrusion detection in wireless sensor networks[C]// Proceedings of the 13th European Wireless Conference. Paris，France，2007

[5] 赵冬梅，马建峰，王跃生. 信息系统的模糊风险评估模型[J]. 通信学报，2007，28(4)：51-56，64

[6] 张小川，李祖枢. 基于人工生命行为选择的智能体决策的研究[J]. 计算机科学，2007，34(5)：213-214，251

[7] Maarouf I. Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks[J]. IET Communications，2009，3(5)：846-858

[8] Jaquith A. Security Metrics：Replacing Fear，Uncertainty，and Doubt[M]. 李冬冬，韦荣，译. 北京：电子工业出版社，2007：22

[9] 包秀国，胡铭曾，张宏莉，等. 两种网络安全管理系统的生存性定量分析方法[J]. 通信学报，2004，25(9)：34-41

(上接第 56 页)

[9] Sewani A. Packet Level Worm Simulation and Analysis[OL]. http://www.cs.berkeley.edu/~anil/papers/worm_sim.ps

[10] http://www.emulab.net

[11] http://www.isi.edu/deter.

[12] http://www.planet-lab.org

[13] Twycross J，Williamson M M. Implementing and testing a Virus Throttle[C]// Proceedings of 12th USENIX Security Symposium. August 2003

[14] Liljenstam M，Yuan Y，Premore B，et al. A mixed abstraction level simulation model of large-scale internet worm infestations [C]//MASCOTS. IEEE，October 2002