文章编号:1671-4598(2017)12-0263-04 DOI:10.16526/j.cnki.11—4762/tp.2017.12.068 中图分类号:TN393 文献标识码:A

模拟复杂网络下子网络节点抗攻击设计

龚小刚,叶 卫,方 舟,王云烨
(国网浙江省电力公司信息通信分公司,杭州 310007)

摘要:针对复杂网络节点受攻击而出现的安全性问题,提出在模拟复杂网络基础上结合Feistel算法的子网络节点抵抗攻击方法;该方法通过子网络节点定位参数集,建立恶意节点位置模型,并确定定位真实精度;而后利用Feistel算法对节点密文进行加密处理,进而使加密信息恢复成明文信息,完成模拟复杂网络下子网络节点的抗攻击方法改进;结果证明,该方法不仅能够准确地对恶意节点进行定位,而且增强了节点抗攻击性能,提升了网络安全性。

关键词:复杂网络;子网络节点;抗攻击;Feistel算法

Simulate the Design of Anti — attack on Network Nodes of Complex Network

Gong Xiaogang, Ye Wei, Fang Zhou, Wang Yunye
(State Grid Zhejiang Electric Power Company Information & Telecommunication Branch, Hangzhou 310007, China)

Abstract: Aiming at the security problem of complex network nodes attacked, a method of resisting attack is proposed for subnet nodes based on Feistel algorithm in the simulation of complex networks. By means of the method of sub network node location parameter set, a malicious node location model, and determine the true positioning accuracy; then using Feistel algorithm of node ciphertext encrypted, and the encrypted information back into plaintext information, improve the anti attack method to simulate network nodes of complex networks to complete immediately. The results show that this method can not only locate the malicious nodes accurately, but also enhance the anti attack performance of nodes and improve the security of the network.

Keywords: complex network; subnetwork node; anti attack; feistel algorithm

0 引言

以Internet为代表的信息技术的迅猛发展代表人类大步迈入了网络时代,社会的网络化是一个双刃剑,既给人们生活带来了生产效率和生活质量,也带来了一些负面影响[1-2]。在复杂网络环境下,难免会出现数据丢失,信息泄露,网络节点受到恶意攻击等现象,为此,应该对子网络节点进行抗攻击设计[3]。当前的子网络节点抗攻击系统的设计方法存在加解密时间长、安全性低、恶意节点定位不准确等问题,容易受到来自外界的攻击,对网络造成了安全隐患。

针对上述问题,用Feistel算法完成子网络节点抗攻击设计。该算法能够根据子网络节点定位参数集,建立恶意节点位置模型,确定真实精度,并对加密与解密进行分析,进而使加密信息恢复成明文信息。通过对网络抗攻击性策略的分析和恶意攻击程度的设定可以计算出衡量算法精准度的标准,并采用对比方法进行实验。实验结果证明,该算法不仅能够加快密钥更新速度,还能准确地对恶意节点进行定位,大大增强了网络安全性,也能为其它网络节点抗击设计提供分析依据。

1 模拟复杂网络拓扑结构

对复杂网络拓扑结构进行模拟,需先掌握复杂网络中拓扑结构的特点。通过对拓扑结构特征量进行统计,来表述复杂网络拓扑结构的特征。拓扑结构的统计特征量主要包括:度、度的分布及度的相关性。其中度的相关性指的是带有某种特定度的网络节点,判断它是否与另一个带有某种特定度的网络节点相连,如若得出两个节点的倾向性为0,则认为这两个网络节点度不相关。换言之,判断两个网络节点之间节点边是否连接,与两节点自身的度毫无关系。

假设网络中有 N 个节点,每个节点对之间的链接概率为 P,则最后产生的 N 个节点的网络模型有 $PN(N-1)/2$ 条边[4]。

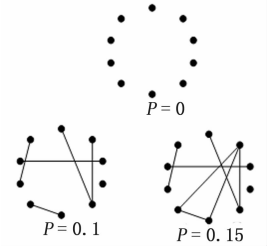

图1 随机复杂网络模型示意图

由随机网络模型的选定概率 P 可知:

1)当 $p=0$ 时,边数为0,网络中所有节点都是孤立的,节点间物相互联系,$<k>=0, C=0, L=o$;

2)当 $p=1$ 时,边数为 $N(N-1)/2$,网络完全连通,所有节点都是最近邻,到网络中任何节点的路径都是1,这种的网络结构开始容易受到攻击,节点之间的关联性会受到影响,从而破坏网络的稳定性。

3)当 p 介于0和1之间时,网络边数介于0和 $N(N-1)/2$ 之间,$<k>=p\{N-1\}, C=p, L=\frac{\ln(N)}{\ln(K)}$。这时网络结

收稿日期:2017-09-04; 修回日期:2017-10-14。

作者简介:龚小刚(1987-),男,浙江金华人,硕士研究生,工程师,主要从事网络与信息安全方向的研究。

构就属于复杂网络，由于其结构较为复杂，节点容易出现混乱现象，所以更容易受到攻击。

一般情况下，复杂网络表示为：

$$Q = W(A,B) \tag{1}$$

其中：A 为网络节点集合；B 为边的集合；W 为节点数量。复杂网络下的抗攻击性结构可以分为最优拓扑结构[4]和构建成本最少的网络拓扑结构[5]，对于系统结构功能来说具有重大的影响，因此将网络拓扑结构下的子网络节点抗攻击设计按照该思路进行研究：

1）最优拓扑结构：

在一定构建成本的条件下，最优子网络节点抗攻击性的网络结构为：

$$F = \max(R \cdot Q)_{\gamma} \tag{2}$$

式（2）中，R 为子网络节点抗攻击性测度；γ 为复杂网络构建成本；Q 为复杂网络结构。

2）构建成本最少的网络拓扑结构：

在抗攻击性一定的条件下，构建成本最少的网络拓扑结构为：

$$\gamma = \min(R \cdot Q)_{F} \tag{3}$$

式（3）中，γ 为复杂网络构建成本；R 为子网络节点抗攻击性测度；Q 为复杂网络结构。

在上述两种拓扑结构中，假设有 i 个子网络节点都存在于网络拓扑结构中，在构建成本一定或者抗攻击性一定的条件下，外部的攻击解密就变得更加容易，对于解密的情况一般分为两种：一种是 64 位的解密方法[6]，另一种就是 128 位的解密方法[7]。在实际情况中，最常用的方法就是使用十个十六进的字符或者五个 ASCII 字符的 64 位解密方法[8]。攻击解密操作都会针对子网络节点进行，但是在设计中加入密钥就可以避免敏感信息的暴露，增强抗网络攻击性，因此，使用 Feistel 算法来完成子网络节点抗攻击的设计。

2 模拟复杂网络下子网络节点抗攻击设计

2.1 Feistel 节点加密算法原理

加密是一种对网络节点设定访问权限的技术。通过秘钥对网络节点进行加密，加密过程中产生的编码成为密文。将密文还原成原始明文的过程称为密钥的解密，也就是对加密的反响处理。加密技术的使用，可使网络节点具有一定的私密性，能够有效防止非法入侵者盗取明文。还具有一定的鉴别性，能够确保网络节点所接受的信息是合法的。此外经过加密的网络节点完整性更高。采用加密技术，充分利用其优势，引入 Feistel 节点加密算法，对 Feistel 节点加密算法原理进行分析，完成模拟复杂网络下子网络节点抗攻击设计。

在复杂网络拓扑结构下，尽可能地减少加密算法所占用的空间，将原来 56 位的密钥改造为 128 位[9]，并将密钥分为四部分，在这四部分中，每一轮都需要使用 32 位密钥进行改造，与此同时，进行转换处理[10]，具体加密过程如图 2 所示。

由图 2（a）可知：在加密的过程中使用轮函数来表示，并且 F、H、CF、CH 都是 32 位的。其中：

$$\begin{aligned} F &= H_{i-1} \\ H &= F_{i-1} + W(H_{i-1},K_i) \\ i &= 1,2,3 \end{aligned} \tag{4}$$

具体的解密过程如图 2（b）所示。

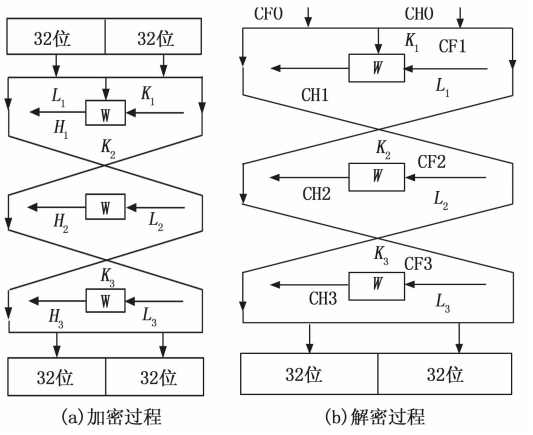

图 2 加解密过程

解密过程的输入就是加密过程密文的输出，由此可以得出：

$$CH_i = F_{i-1} \tag{5}$$

如果 $F_{3-i+1} = H_{3-i}$ 的存在，那么必然有 $CH_{i-1} = H_{i-1}$，当 $i = 4$ 的时候，$F_0 = CH_3$，$H_0 = CF_3$，此时加密的信息就可以完全恢复成明文信息，从而完成密文的加密处理，抵抗恶意攻击，提高了网络安全性能。

2.2 基于 Feistel 算法完成子网络节点抗攻击设计

对子网络节点抗攻击设计的过程中，首先需要确定攻击子网络节点的定位，建立恶意节点位置模型，确定真实精度；然后利用 Feistel 算法对密文进行加密处理，从而加快密钥更新速度，抵抗恶意攻击，提高网络安全性。

子网络节点的定位主要与参数集：$X = \{(a_1,b_1,Y_1),(a_2,b_2,Y_2),\cdots,(a_m,b_m,Y_m)\}$ 有关，其中：(a_m,b_m) 表示的是第 m 个恶意攻击的位置到节点的距离。恶意节点通过改变 (a_m,b_m) 值来缩短与节点之间的距离，显示虚假位置，直到完成攻击。当子网络节点需要从 A 向 B 发送数据包时，恶意节点 N 也会拦截数据包，并释放干扰，导致 B 点不能接收到 A 点所发送的数据，此时扩大 Y_m 值，N 拦截来自子网络节点 A 的数据包将会被延迟，并利用 Feistel 算法确定恶意攻击的位置，建立恶意节点位置模型，如图 3 所示。

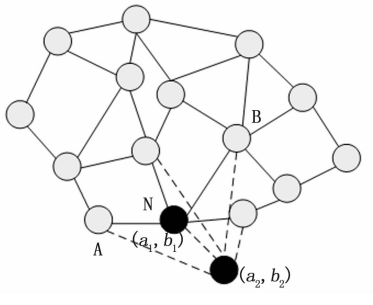

图 3 恶意节点位置

由图 3 可知，恶意节点 N 的实际坐标为 (a_1, b_1)，但是显示的虚假位置为 (a_2, b_2)，这种情况下的恶意节点 N 实现定位的精度将会受到影响。假设恶意节点占全部节点的比例为 p，全部子网络节点为 M 个，那么从 M 个子网络节点中选

择出 N 个的节点组合为：$D = C_M^N$，选择组合方案后，利用公式（4）确定两个节点之间的距离，并对节点进行定位，对于待定节点的坐标，可以使用预测坐标替代真实定位进行精度的计算：

$$E = \frac{(Y_m - \sqrt{(a_j - a_1)^2 + (b_j - b_1)^2})}{N}, j = 1,2,\cdots,D \quad (6)$$

式（6）中，(a_j, b_j) 为选择第 j 种方案的子网络节点坐标，确定攻击子网络节点的定位，并得出定位的精度。由上述过程完成虚拟复杂网络下子网络节点抗攻击方法是设计。

根据以上步骤，完成了模拟复杂网络下网络节点抗攻击设计。

3　实验分析

对模拟复杂网络下子网络节点抗攻击设计中定位的准确性、加密解密时间、安全性方面进行了实验，为了确保实验的真实性和准确性，在公开数据的实验平台上进行了检验，并确认恶意攻击只对子网络节点攻击的情况下，对实验数据进行收集，允许实验误差范围在 5%以下。

3.1　参数设定

为了保证本文采用的 Feistel 算法完成子网络节点抗攻击设计的有效性，对参数进行设定。根据网络抗攻击性策略的分析（如表 1 所示）。

表 1　网络抗攻击性类别分析

类别	节点冗余	中继节点	无标度网络
网络延时	无现象	降低	无现象
生存周期	降低	上升	无现象
建设成本	无现象	增加	无现象
环境适应情况	强	一般	强
攻击类别	随机性	被选择性	组织性

表 2　恶意攻击程度

参量	数值
节点	40 个
攻击次数	100 次
攻击间隔时间	5s
攻击范围	每次 1 个节点
攻击效果	每次丢失 5 个数据包

3.2　节点定位准确度结果与分析

任何一个节点都在其余节点的通信范围内，选择 4 种节点作为信标节点，并对其余的节点进行定位。由普通节点与信标点之间的信号值可以通过计算得到这 4 个信标点的估计距离，利用估计距离对其余的普通节点进行定位。假设第 i 个普通节点的定位能够得到最优的位置 (a'_i, b'_i)，计算该位置与实际位置 (a_i, b_i) 之间的距离的误差为：$S'_i = \sqrt{(a'_i - a_i)^2 + (b'_i - b_i)^2}$，将该距离作为第 i 个普通节点的估计误差，由表 2 可知，设定的普通节点有 40 个，由此可得出平均误差：$S'' = \frac{1}{40}\sum_i S'_i$，该误差可以作为衡量算法精准度的标准。

将传统算法与改进算法网络恶意攻击节点定位准确度进行对比，得到两种算法恶意攻击节点定位准确度对比结果如图 4 所示，其中黑色实心圆圈代表准确定位节点，空心圆圈代表偏离定位节点。

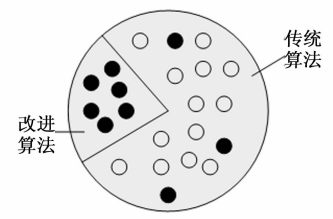

图 4　两种算法节点定位准确度对比情况

由图 4 可以看出：采用传统算法进行网络恶意攻击节点定位，本次实验共进行 16 次恶意攻击节点定位，其中偏离定位节点有 13 个，准确定位节点却只有 3 个，可求出传统算法的节点定位准确度为 28%。采用改进算法对网络恶意攻击节点进行定位，实验中近乎全部节点均为准确定位节点，其节点定位准确度高达 99%。对比两种算法的节点定位准确度，明显看出改进算法所获取的恶意攻击节点定位比较准确，恶意攻击节点定位率为 99%，而传统算法所获取的恶意攻击节点定位较差，恶意攻击节点定位率为 20%左右，很难准确的将恶意节点定位，使得传输的数据包大量的丢失，造成了子网络节点抗攻击能力降低。实验结果充分说明，改进算法对网络恶意攻击节点进行定位的准确度更高，验证了改进算法的有效性。

3.3　加解密结果与分析

根据表 2 可知，本次实验所发起的攻击次数为 100 次，生成密钥的过程中，会受到不同程度的攻击频率，且随着时间的增加，攻击频率也逐渐的增强，当攻击频率较大时会影响密文的加密过程。分别利用文中的 Feistel 算法（改进算法）、文献[8]算法和文献[9]算法，对密钥生成情况进行监测，攻击的频率随着时间的变化发生了改变，对比三种不同算法在密钥生成过程中受到攻击的频率，得到三种算法攻击频率对比结果如图 5 所示。

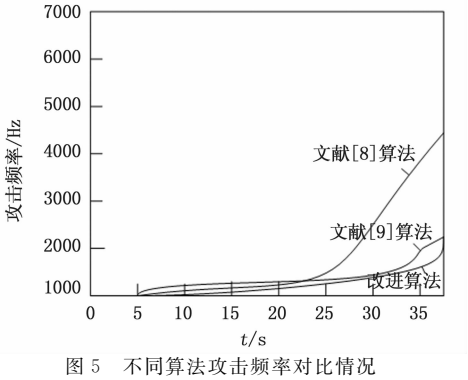

图 5　不同算法攻击频率对比情况

由图 5 可知：利用文献[8]算法对密钥生成过程进行监测，其攻击频率随着时间的增加大幅度增大，当时间为 24 s 时，受到攻击频率明显增大，并呈急剧上升趋势。当时间为 35 s 时，攻击频率达到最大值为 4 800 Hz。采用文献[9]算法对密钥生成过程进行监测，其攻击频率随时间上升速度缓慢，在时间为 34 s 时，受到攻击频率加剧，当时间为 35 s 时，所受攻击频率达到最大值为 2 100 Hz。利用 Feistel 算法，即改进算法对密钥的生成过程进行监测，其攻击频率曲线十分平

缓，当时间为 35 s 时，受到攻击频率才出现较大增长，同时也是攻击频率达到最大值的时刻，最大值为 1 800 Hz. 对比三种不同算法进行密钥生成情况监测时，所受攻击频率的情况，看出文献［8］算法受攻击频率最大，其稳定性较差。文献［9］算法相比文献［8］算法，其受攻击频率较低，稳定性有所提高，但提高效果并不明显。改进算法受攻击频率远远小于文献［8］算法和文献［9］算法的受攻击频率，且受攻击频率随时间的增大变化很小，实验结果充分表明，改进算法的受攻击频率低，稳定性高，验证了改进算法的实用性。

以上通过对密钥加密过程的受攻击频率进行测试，来验证 Feistel 算法的稳定性。在密钥的解密过程中，解密时间的大小也是验证 Feistel 算法性能的一项重要指标。以下实验对密钥解密过程中的解密时间进行测试，用以验证 Feistel 算法的执行速率。因此，分别采用传统算法与改进算法对密钥解密过程进行监测，测试两种算法的解密时间，得到两种算法解密时间对比结果，如图 6 所示。

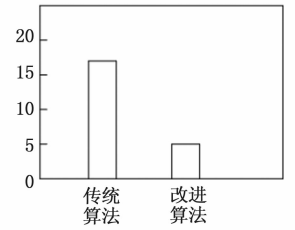

图 6 两种算法加解密时间对比

观察图 6 可知，采用传统算法对密钥解密过程进行监测，其解密时间达到了 17 s，采用改进算法对密钥解密过程进行监测，其解密时间为 5 s。对比改进算法和传统算法的解密时间，改进算法的解密时间仅仅是传统算法解密时间的三分之一。实验结果表明，改进算法的解密时间少，其执行速率更高，验证了改进算法的实用性。

Feistel 算法的抗攻击性与密钥生成解密过程中的加解密耗时有直接的关系。为了验证 Feistel 算法的抗攻击性，分别对改进算法和传统算法的进行测试。分析两种算法的加解密耗时与抗攻击次数情况，得到两种算法抗攻击性对比结果如表 3 所示。

表 3 两种算法抵抗攻击对比情况

	耗时/s	攻击次数	抗攻击次数
传统算法	17	100	95
改进算法	5	100	65

由上述分析可知：通过迭代次数与加密解密时间的对比情况可以明显的看出，采用传统算法对密钥加解密过程进行监测，其加解密耗时为 17 s，过程中共收到 100 次攻击，抗攻击次数为 95 次。通过实验数据可知，应用传统算法监测的密钥加解密过程，在抵抗攻击方面耗费大量精力，导致加解密时间长，执行速率较低。采用改进算法对密钥加解密过程进行监测，其加解密耗时为 5 s，过程中共收到 100 次攻击，抗攻击次数为 65 次。观察实验数据可得，改进算法在抵抗攻击方面耗费较少，因此其加解密耗时较少，执行速率大幅度提高。对比改进算法与传统算法所使用的加解密时间，缩短了将近 3 倍，改进算法的执行速率明显提高。对比改进算法与传统算法的抗攻击次数，相同攻击情况下，改进算法的抗攻击次数仅是传统算法的一般，说明改进算法大大提高了抗攻击能力，其抗攻击性稳定在 95％左右，大于传统算法抗攻击性的 30％左右。实验结果充分表明，改进算法的加解密耗时小，抗攻击性高，利用改进算法能够有效的提高密钥生成的安全性，使抗攻击设计能够在实时性、安全性的方面达到一种相对稳定的状态。

3.4 实验结论

由上述实验过程可以得出实验结论：通过对网络抗攻击性策略的分析和恶意攻击程度进行设定可以计算出衡量算法精准度的标准，通过标准将传统算法与改进算法节点定位准确度进行对比，可以看出改进算法恶意攻击节点定位率较高。通过采用改进算法和传统算法对密钥加解密过程进行监测，得到改进算法在密钥加密时受攻击频率低，在密钥解密时解密时间短，在整体加解密过程中，加解密耗时少，抗攻击性强。以上实验结果表明，所提的 Feistel 算法节点定位准确度高，稳定性高、执行速度快、抗攻击性强，具有一定的实用性和有效性。同时，改进算法还能够提高复杂网络的安全性，能为其它网络节点抗击设计提供分析依据。

4 结束语

为解决传统复杂网络中节点受攻击造成网络不安全的问题，提出基于 Feistel 算法完成子网络节点抗攻击设计。该设计方法通过子网络节点定位参数集，构建恶意节点位置模型，利用 Feistel 算法对节点密文进行加密处理，完成模拟复杂网络下子网络节点的抗攻击设计。实验结果证明，改进设计的使用能够准确的对恶意节点进行定位，执行效果较强，使用该算法还能大幅度的缩短运算时间，使抗攻击设计能够在实时性、安全性的方面达到一种相对稳定的状态。但该设计方法尚有不足之处，面对网络结构复杂化的发展趋势，节点抗攻击问题还需继续研究，以便为日后网络安全做准备。

参考文献：

[1] 黄玉划，代学俊，时阳阳，等. 基于 Feistel 结构的超轻量级分组密码算法（PFP）[J]. 计算机科学，2017，44（3）：163－167.
[2] 张博亮，钟卫东，杨晓元. 物联网环境下 Feistel 结构分组密码的差分故障分析 [J]. 应用科学学报，2016，34（5）：547－554.
[3] 代学俊，黄玉划，刘宁钟. 基于双伪随机变换和 Feistel 结构的轻量级分组密码 VHF [J]. 计算机科学，2017，44（2）：192－194.
[4] 孙 昱，姚佩阳，张杰勇，等. 基于优化理论的复杂网络节点攻击策略 [J]. 电子与信息学报，2017，39（3）：518－524.
[5] 王甲生，吴晓平，陈泽茂，等. 修复策略下典型拓扑结构复杂网络抗毁性研究 [J]. 海军工程大学学报，2015，27（4）：75－79.
[6] 冯慧芳，李彩虹. 基于复杂网络的车载自组织网络抗毁性分析 [J]. 计算机应用，2016，36（7）：1789－1792.
[7] 郑文强，陈云翔，庄 骏，等. 基于复杂网络理论的航材配送网络抗毁性分析 [J]. 火力与指挥控制，2015（2）：128－132.
[8] 沈亦军，钟伯成. 一种入侵者视野下的复杂网络安全评估方案 [J]. 计算机工程与应用，2015，51（15）：119－123.
[9] 王 伟，刘付显，邢清华. 基于复杂网络的作战同步建模与优化 [J]. 火力与指挥控制，2016，41（12）：91－95.
[10] 陈植林，蔡晓霞，陈 红，等. 战术互联网子网干扰效果评估 [J]. 火力与指挥控制，2016，41（4）：126－130.