

# 计算机网络入侵环境下健康节点通信选择算法的研究与仿真

胡 艳

(广西财经学院, 广西 南宁 530003)

**摘 要:** 提出一种新的网络入侵环境下健康节点通信选择算法, 依据网络入侵数据的特点, 引入统计学中分类思想实现网络入侵数据的检测. 在此基础上, 给出健康节点通信失真表达式, 采用最靠近信源的健康节点通信选择方法, 使其他节点进入休眠模式, 并对失真情况进行分析. 选择一定范围内的健康节点进行数据传输, 依据计算结果与失真误差要求对范围进行划定, 从而实现健康节点通信选择. 实验结果表明, 所提算法不仅失真性低, 能够保持传输信息的完整性和通信安全, 而且所需能耗低, 通信效率高.

**关键词:** 网络入侵环境; 健康节点; 通信; 选择

**中图分类号:** TN925

**文献标识码:** A

**文章编号:** 1000-7180(2017)01-0141-04

## Under the Environment of Network Intrusion Health Node Selection Algorithm in the Research and Simulation of Communication

HU Yan

(Guangxi University of Finance and Economics, Nanning 530003, China)

**Abstract:** Put forward a new network intrusion environment health communication node selection algorithm, based on the characteristics of the network intrusion data, the introduction of statistical classification thought realize network intrusion detection of data. On this basis, gives health node communication distortion expression, use the most close to the health of the source node communication method, make the other nodes into sleep mode, analyzes methods cause the distortion of the situation. Select nodes for data transmission to a range of health, on the basis of calculation results and the distortion error requirement to delimit the scope of nodes so as to realize healthy choice for communication. The experimental results show that the proposed algorithm not only true loss is low, can maintain the integrity of the information transmission and communication security, and the low energy consumption, high communication efficiency.

**Key words:** network intrusion environment; health node; communication; choice

### 1 引言

近年来,随着计算机和网络的逐渐发展,人们对网络安全性和通信效率的要求越来越高<sup>[1-3]</sup>. 网络受到入侵时,为了保证整个网络的鲁棒性和监测信息的准确性,需设计一种有效的健康节点通信选择方法,以减少传输数据量,减缓网络拥塞<sup>[4-6]</sup>.

文献[7]提出一种基于分布式 Alamouti 编码的健康节点通信选择算法,该算法通过分布式时空编码形式实现健康节点通信选择,实现过程简单,但其

选用的健康节点间协作通信方式不佳,导致通信效率低下;文献[8]提出一种基于非盲流水印的健康节点通信选择算法,该算法针对网络入侵者易于占据匿名链路出入口的问题,通过对健康节点进行加权处理实现健康节点通信选择. 该算法能够提高节点通信安全性,但实现过程过于复杂,容易出现误差;文献[9]令所有节点对其余节点传输数据包的次数和通信协作时节点的中继策略进行监测记录,将传输次数最少的节点作为下一次通信需选择的节点. 该方法能够降低竞争接入时间,但节点能耗较多;文

献[10]提出一种基于随机带宽加权的健康节点通信选择算法,该算法依据带宽大小对健康节点进行排列分组,在进行节点通信选择时引入随机因素提高通信安全性.该算法不仅实现过程简单,而且安全性很高,但其存在通信效率低的弊端.

针对上述算法的弊端,提出一种新的网络入侵环境下健康节点通信选择算法,依据网络入侵数据的特点,引入统计学中分类思想实现网络入侵数据的检测.

## 2 网络入侵环境下健康节点通信选择算法研究

### 2.1 网络入侵数据检测

分类是统计学中用来对基础数据进行分析的一种常用方法.本节依据网络入侵数据的特点,引入统计学中分类思想实现网络入侵数据的检测.

假设网络中各个入侵数据组成的集合用  $z_j$  表示,与之对应的权值系数用  $b_j$  表示,那么上述数据需要满足式(1):

$$\sum_{j=1}^p z_j b_j = 1, b_j > 0 \quad (1)$$

运用式(2)求出网络数据库中入侵数据特征的极大值:

$$\sum_{j=1}^p b_j - \frac{1}{2} \sum_{j,k=1}^p b_j b_k z_j z_k l(y, y_j) \quad (2)$$

式中,  $l(y, y_j)$  用于描述核函数;  $z_k$  用于描述网络中正常数据构成的集合,  $b_k$  用于描述与之对应的权值系数.

运用式(3)对网络数据库中入侵数据进行二次规划:

$$z(y) = \text{sign} \left( \sum_{j=1}^p \beta_j z_j l(y_j, y) + c \right) \quad (3)$$

式中,  $\beta_j$  用于描述分类函数;  $c$  代表正常数.

运用式(4)对网络数据中入侵数据二次规划进行对偶规划:

$$\begin{cases} \max \sum_{k=1}^m \beta_j - \frac{1}{2} \sum_{j=1}^m \sum_{k=1}^m z_j z_k \beta_j \beta_k (y_j y_k) \\ \text{s. t. } \sum_{k=1}^m z_k \beta_j = 0 \\ 0 \leq \beta_j \leq y_k \quad k = 1, 2, \dots, m \end{cases} \quad (4)$$

运用上述公式进行一系列后分析后,将网络入侵数据检测问题转化为求解二次规划的对偶规划问题,运用式(5)求出最优解:

$$\beta^* = (\beta_1^*, \beta_2^*, \dots, \beta_m^*)^T \quad (5)$$

式(6)表示最优分类函数:

$$g(y) = \text{sgn} \{ (x^* y) + c \} \quad (6)$$

运用以上方法,对网络中的入侵数据进行降维处理,从而降低冗余数据.根据网络入侵数据特点,使用最优分类函数完成对其的分类处理,进而达到检测网络入侵数据的目的.

### 2.2 健康节点通信选择算法

在网络入侵数据检测的基础上,本节分析健康节点通信选择算法.在网络中分布着大量节点,当所有节点都在传输数据时,势必会引起因信号碰撞带来的时间延迟和能量浪费,造成节点通信过程中资源的不充分利用.因此,本节在入侵节点被检测完成的环境下,在实现健康节点通信选择的同时,尽可能保证健康节点传输信息不失真和资源的充分利用.

健康节点间的距离与信源靠近程度息息相关.健康节点间距离越近,相关系数越大.越靠近信源的健康节点的感知数据越接近信源.因为健康节点针对同一信息采用相同的处理过程和衰落延迟方式,所以在接收端得到的原始信号  $Z_1 Z_2 \dots Z_i \dots Z_N$  间都有相似关系,但是  $Z_j$  包含信息量不如  $Z_i (i < j)$  丰富.

由于距离信源越近的健康节点传回的信息越有价值,所以当某个需要监测的事件发生时,通常选用距离其最近的健康节点传回的信息,而不是距离其较远的健康节点,从而使接收端接收信息后更易恢复事件的信源.

健康节点通信失真表达式如下:

$$D_e = \sigma_s^2 - \frac{\sigma_s^2}{N(\sigma_s^2 + \sigma_N^2)} (2 \sum_{i=1}^n p_{si} - 1) + \frac{\sigma_s^2}{N^2(\sigma_s^2 + \sigma_N^2)^2} \sum_{i=1}^N \sum_{j \neq 1}^N p_{ij} \quad (7)$$

式中,  $\sigma_s^2$  用于描述事件信息的方差;  $N$  用于描述健康节点数量;  $\sigma_N^2$  用于描述观测噪声的方差;  $p_{si}$  用于描述信源与任意健康节点间的相关系数;  $p_{ij}$  用于描述两个健康节点间的相关系数.

若需要选取  $M$  个健康通信节点,只需将式(7)中的节点值  $N$  转换成  $M$ .此外,失真程度只取决于两个相关系数  $p_{si}$  和  $p_{ij}$ .其中  $p_{si}$  对失真程度呈正影响,  $p_{ij}$  对失真程度呈负影响.选择更靠近信源发生地的健康节点就可使被选中的健康节点具有更大的  $p_{si}$  值;换言之,选择远离信源发生地的健康节点就可使被选中节点具有更大的  $p_{ij}$  值.通过以上分析可知,如果能选取一个最靠近信源发生地的健康节点进行通信,令其它健康节点不发送数据,就可使  $p_{si}$

值最大而  $p_{ij}$  值最小,在这种只需一个健康节点通信的特殊情况下,通信将大大减少,从而达到减少能耗和降低时延的目的。

综上所述,本节采用最靠近信源的健康节点通信选择方法,使其他节点进入休眠模式。

下面求出因上述分析方法造成的失真,当健康通信节点降低为一个时,接收端依旧通过相似技术对信源进行估计,计算出失真值,公式描述如下:

$$D_k = \sigma_s^2 - \frac{2\sigma_s^2 p_{sk} - \sigma_s^4}{\sigma_s^2 + \sigma_N^2} \quad (8)$$

比较式(8)与式(7),发现  $D_k$  比  $D_e$  只少一项  $p_{ij}$ ,二者间的差异较小。

由此可见,利用最靠近信源的单个健康节点进行通信,较采用远离信源的健康节点通信和选择任意健康节点通信性能更优越。在理想状态下,选择距离最短的健康节点通信性能最好。但实质上,判断健康节点是否是距离信源最短的节点很难。针对实际应用,若计算结果在允许误差范围内,那么对于某个具体的应用,选择一定范围内的健康节点进行数据传输将非常有效,这时上述节点范围的划定将非常关键,下面进行详细的分析。

实质上,每个系统都有自己的可靠性和失真性要求,因此针对某个具体实际应用,健康节点通信选择只需要满足系统可靠性和失真性要求即可。通过数学分析可知,假定选择健康节点  $n_k$  通信,因为失真值  $D_k$  取决于健康节点与信源间的距离  $d_{sk}$ ,所以若需将失真值控制在  $D_0$  范围内,此时距离  $d_{sk}$  需满足以下条件:

$$D_k = \sigma_s^2 - \frac{2\sigma_s^2 p_{sk} - \sigma_s^4}{\sigma_s^2 + \sigma_N^2} < D_0 \quad (9)$$

式中,  $p_{sk}$  用于描述信源与该健康节点间的相关系数。

综上可知,在选择健康通信节点时,在将信源发生地作为圆心,将  $D_0$  作为半径的圆范围内,将该圆范围内的任意节点集合在一起,只要健康节点参与通信后被接收端接收,计算结果与失真值都在误差允许区间中,那么在进行通信时,只需在上述集合中任选一个健康节点,就可以满足系统对失真性的要求。

### 3 仿真实验结果分析

为了验证本文提出方法的有效性,需要进行相关的实验分析。实验将随机加权算法、蚁群算法作为对比进行测试。本文进行仿真实验和分析时所用的

数据是 Tor 网络在线节点的真实数据。在进行仿真时 Tor 网络共有节点 1 584 个,其中入/出口节点分别为 420 个和 554 个。

#### 3.1 失真性能测试

在  $45 \times 45$  的 Tor 网络中共有 400 个节点,在该范围内将信源  $n_0$  坐标  $(x_0, y_0)$  看作原点,依据与  $n_0$  距离的大小对健康节点进行排序。图 1 描述的是本文算法、随机加权算法、蚁群算法失真性比较结果。

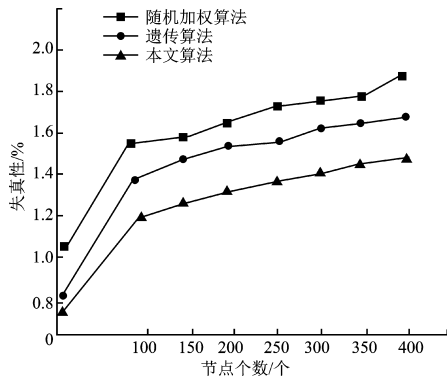


图1 三种算法失真性比较结果

分析图1可以看出,随着节点数量的逐渐增加,本文算法、遗传算法和随机加权算法的失真性均逐渐增加,运用本文算法得出的失真值明显低于遗传算法和随机加权算法,说明本文算法的失真性最低,最能保持信息的完整性。

#### 3.2 安全性测试

为了测试本文算法的安全性,将遗传算法、随机加权网络算法作为对比,以概率累计值  $F(X)$  为安全性评价指标。概率累计值就是之前所有健康节点的安全性累计值,概率累计值越高,安全性越高。三种方法的概率累计值  $F(X)$  比较结果用图2进行描述。

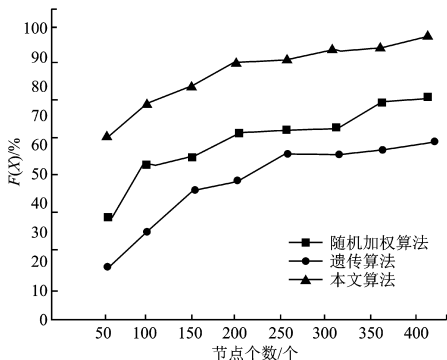


图2 三种算法安全性比较结果

分析图2可以看出,针对不同的攻击节点数量,本文算法的概率累计值一直明显高于遗传算法和随

机加权网络算法,说明和其他两种算法相比,采用本文算法对健康通信节点进行选择更能保证通信的安全性.

3.3 节点剩余能量测试

节点剩余能量是节点通信时耗费能量均匀性的体现,节点剩余能量越高,则通信时耗费能量越少.图 3 描述的是随着时间的变化,本文算法、遗传算法和随机加权算法的节点剩余能量变化情况.

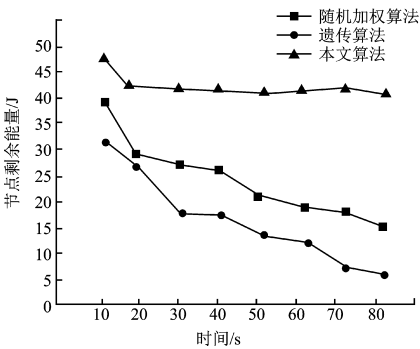


图 3 节点剩余能量变化情况

分析图 3 可知,在网络工作时间逐渐增加的情况下,遗传算法和随机加权网络算法的最小剩余能量一直高于本文算法的最小剩余能量,且整体看来,遗传算法的剩余能量曲线高于随机加权网络算法,而本文算法的节点剩余能量明显高于遗传算法和随机加权网络算法.这就表示,和其它两种算法相比,本文算法能更加均匀的消耗各节点能量.

3.4 延迟时间和通信时间测试

在网络中,延迟时间(latency)就是从某健康节点得到一个数据包所需的时间;通信时间就是健康节点传输一个数据包所需的时间,延迟时间和通信时间越低,则健康节点通信效率越高.表 1 描述的是采用本文算法、遗传算法和随机加权网络算法的延迟时间、通信时间比较结果.

分析表 1 可以看出,遗传算法的延迟时间低于随机加权网络算法,而本文算法的延迟时间明显低于遗传算法和随机加权网络算法.且针对通信时间,本文算法也明显低于其他两种算法,这主要是因为遗传算法和随机加权网络算法的节点的剩余能量较低,导致节点竞争延迟时间增多.说明本文算法具有较高的通信效率.

4 结束语

本文提出一种新的网络入侵环境下健康节点通信选择算法,实验结果表明,所提算法不仅失真性低,

表 1 三种算法通信效率比较结果

| 实验<br>序号 | 本文算法        |             | 遗传算法        |             | 随机加权<br>网络算法 |             |
|----------|-------------|-------------|-------------|-------------|--------------|-------------|
|          | 延迟时<br>间/ms | 通信时<br>间/ms | 延迟时<br>间/ms | 通信时<br>间/ms | 延迟时<br>间/ms  | 通信时<br>间/ms |
| 1        | 3.22        | 4.17        | 5.17        | 6.11        | 6.35         | 8.16        |
| 2        | 2.93        | 4.59        | 5.26        | 6.07        | 6.96         | 9.34        |
| 3        | 2.89        | 4.24        | 5.34        | 6.28        | 7.22         | 8.85        |
| 4        | 3.04        | 4.94        | 4.98        | 6.33        | 7.39         | 9.22        |
| 5        | 3.15        | 3.83        | 6.13        | 6.45        | 6.71         | 9.43        |
| 6        | 3.11        | 5.11        | 5.84        | 7.16        | 6.92         | 8.67        |
| 7        | 2.97        | 5.06        | 5.96        | 7.39        | 7.44         | 8.52        |
| 8        | 3.14        | 4.73        | 5.73        | 6.82        | 7.36         | 9.06        |
| 9        | 2.88        | 4.92        | 6.17        | 7.44        | 7.81         | 8.75        |
| 10       | 3.19        | 4.58        | 5.29        | 7.29        | 7.33         | 9.11        |

能够保持传输信息的完整性和通信安全,而且所需能耗低,通信效率高.

参考文献:

[1] 王章静,张琦,罗俊海.无线传感网络通信优化仿真分析[J].计算机仿真,2014,31(1):282-285.

[2] 陈志泊,张蕾蕾,李巨虎,等.基于入侵杂草优化算法的无线传感网节点定位[J].计算机工程与应用,2014,50(9):77-82.

[3] 左毅,陈勇,游华.网络入侵应急模型快速响应方法研究与仿真[J].计算机仿真,2014,31(2):358-361.

[4] 章治.无线传感网络少量节点入侵评估模型仿真[J].计算机仿真,2014,31(4):318-321.

[5] 李振刚,甘泉.改进蚁群算法优化 SVM 参数的网络入侵检测模型研究[J].重庆邮电大学学报(自然科学版),2014,26(6):785-789.

[6] 李骏骁.多层差异网络深度入侵数据挖掘方法研究[J].计算机仿真,2015,32(4):235-238.

[7] 史望聪,耿健.计算机网络路由选择中改进量子进化算法的应用[J].电子设计工程,2016,24(9):45-47.

[8] 陈拥军,徐罡,周兴付,等.无线传感器网络最少数量通信节点定位方法[J].计算机工程与应用,2014,50(5):55-59.

[9] 李向丽,艾文君.一种基于通信节点身份认证的安全绑定机制的研究[J].计算机应用与软件,2015,32(1):294-296.

[10] 李纪伟,张凯龙,张大方,等.实时工业以太网无线通信节点的设计与实现[J].计算机工程与应用,2015,51(15):112-118.

作者简介:

胡 艳 女,(1979-),硕士研究生,讲师.研究方向为软件工程与数据处理. E-mail:hustgcrao@163.com.