中文核心期刊

光纤网络被入侵后移动中继节点动态分布选取算法

马顺利，乜国雷，叶 涛，刘 昕
（青海民族大学 计算机学院，西宁 810007）

摘要：光纤网络被入侵后，通过合理地选择节点可以在不加外部资源的条件下保证网络正常通信，但入侵的随机性给节点选择带来了困难。针对此问题，提出光纤网络在恶意数据入侵下移动中继节点动态分布选取算法，根据光纤网络硬件结构特点，在入侵约束条件下，建立基于映像的节点集群部署模型；消除入侵随机性带来的干扰，给出了移动中继节点选取的约束条件，结合光纤网络现有节点间的欧式距离和节点损坏情况，确定中继节点的可用数量和最优位置，提高光纤网络在入侵下的网络覆盖率和链路性能。实验结果表明，提出的移动中继节点分布系统设计可以有效改善光纤网络被入侵后的通信性能、提高网络的安全性。

关键词：光纤；传感网络；入侵；中继节点；分布选取
中图分类号：TN911　　**文献标识码**：A　　**文章编号**：1002-5561(2018)05-0041-04
DOI：10.13921/j.cnki.issn1002−5561.2018.05.011

Dynamic distribution selection algorithm for post mobile relay nodes after optical fiber network instrusion

MA Shunli, NIE Guolei, YE Tao, LIU Xin
(School of Computer, Qinghai Nationalities University, Xining 810007, China)

Abstract: When the optical fiber network is invaded, the network can communicate normally without the external resource, but the randomness of the intrusion makes it difficult to select the nodes. The malicious data intrusion fiber network, mobile relay nodes are randomly distributed to the algorithm, based on the hardware characteristics of the optical fiber network, intrusion in the environment, the establishment of a deployment model based on node cluster image; eliminate randomness, mobile relay selection constraints are given, combined with Euclidean distance and node existing fiber network between damage sure, the number of available relay nodes and the optimal position, improve the network intrusion in the optical fiber network coverage and link performance under. The experimental data shows that the proposed mobile relay node distribution system design can effectively improve the communication performance of the optical fiber network after invasion and improve the security of the network.

Key words: optical fiber; sensor network; intrusion; relay node; distribution selection

0 引言

光纤网络作为新兴的网络技术，近年来获得了较快的发展，并在雷达探测、航空侦查、目标跟踪、大气监测、地震救援等诸多关键领域有着十分广泛的应用[1]。光纤网络节点体积小，并且能量多由电池提供[2]，链路连接的稳定性会受到一定影响，而光纤网络的带宽和数据传输量都较大，各种恶意的数据、代码会趁机发动攻击[3,4]。传统针对恶意网络攻击的基于光纤布喇格光栅振动传感入侵识别与检测系统或方法，如免疫模型系统、BP 神经网络算法和数据挖掘算法等均需要较为完备的外设或较长的训练时间，对于光纤网络的安全保护效果不佳[5]。本文提出光纤网络恶意数据入侵下移动中继节点随机分布选取算法，通过对光纤网络节点间串扰攻击进行研究[6]，在光纤网络中选取中继节点，以此改善网络的监控性能和防御性能[7,8]。

收稿日期：2017−09−07。
基金项目：青海省自然科学基金(2017−ZJ−912)资助；“青海省高寒地区智慧畜牧业监测网可信感知节点关键技术研究”资助。
作者简介：马顺利(1970−)，男，硕士，讲师，主要研究领域为密码学与代数组合。

1 信噪比约束参数的设计

我们结合光纤网络多节点的特点，分析节点在入侵环境下的死亡流程，得出在入侵环境下节点死亡流程图，如图 1 所示。

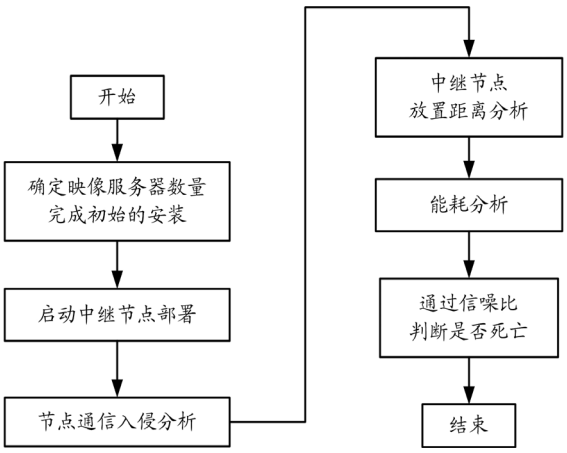

图 1 中继节点入侵后的死亡流程图

光纤网络在通信过程中，由源节点、目标节点和适当数量的中继节点组合而成[9]。为了保证入侵后网络的安全性，对中继点的选位和数量控制十分重要，中继节点的放置位置不能造成网络中其它节点被入侵[10]，其中信噪比是最为重要的参数，该参数设计方法如下：

设计光纤网络的复用因子，计算第 i 个节点的死亡发生率、计算第 i 个节点和第 j 个节点之间的距离，根据经验设定损坏因子，可以计算光纤网络的干扰行为约束模型。如果节点间的入侵干扰来自负责协同传输的邻近中继节点，在已知内部干扰参数，这时建立的光纤网络中的源节点、部署的中继节点以及入侵的行为模型是可以计算的[6]。源节点与中继节点、中继节点和目标节点间相应的信噪比可以计算得出，其入侵干扰程度由采集得到的噪声强度决定，中继节点和目标节点接收的信噪比约束参数 $SINR_1$ 和 $SINR_2$ 可以分别表示为：

$$\begin{cases} SINR_1=\dfrac{|W_{ij}|^2 d^{-\alpha}_{ij}}{N_0+\tau(i,j)} \\ SINR_2=\sum\limits_{i,j\in n}\dfrac{\zeta_0|F_{ij}|^2}{N_0+\tau(d)} \end{cases} \tag{1}$$

其中，W_{ij} 为中继节点 (i,j) 能耗参数，$d^{-\alpha}_{ij}$ 为中继节点的距离参数，N_0 为调整参数（一般情况下为 1），$\tau(i,j)$ 为噪声与距离整合函数。

2 最优节点选取算法设计

确定入侵后中继节点的最佳选取位置，首先考虑在节点信噪比约束符合要求的前提下，中继节点与源节点及目标节点间的欧式距离是否符合要求[11]。在光纤网络组成的空间中，计算任意 2 个节点间的欧式距离 D_{ij}。光纤网络中继节点间的欧式距离采用可分性较好的样本数据进行描述，数据样本的类别不同距离较远[12]，而类别相同则中继节点的样本数据越集中。本文设计一种多赋权方法对部署中继节点的最佳距离进行判定，一组数据的标准差与均值的商值即为这组数据的变异系数，数据集合为 $X=\{x_1,x_2,\cdots\cdots,x_n\}$，则变异系数 λ 的求解过程如下：

$$\lambda=\frac{\xi}{|x_i|} \tag{2}$$

其中，$\xi=\left(\dfrac{1}{n-1}\sum\limits_{i=1}^{n}(x_i-\overline{x})^2\right)^{\frac{1}{2}}$，$\overline{x}=\dfrac{1}{n}\sum\limits_{i=1}^{n}x_i$，。部署中继节点时还要综合考虑到节点间的干扰问题。设 E_s 和 E_r 分别为在 D_{ij} 距离内发送和接收 1bit 数据所耗费的能量，则 E_s 和 E_r 可以表示为：

$$\begin{cases} E_s=E'+E''D^n_{ij} \\ E_r=E' \end{cases} \tag{3}$$

其中，E' 为节点电路部分的干扰，E'' 为第 i 个节点发送射频时的干扰。部署中继节点要能够接收上一跳的数据，经过中继节点的转发而传输到下一跳，此时中继节点 P_i 的干扰为：

$$E_p=E_s+E_r=2E''+E'D_{ij} \tag{4}$$

此时，光纤网络中的源节点 S_i 只负责数据信息的发送，其消耗情况满足 $E_{si}=E_s$；而目标节点 Q_i 只负责接收中继节点传输过来的数据，所以目标节点能耗约束为 $E_{Qi}=E_r$。如果从源节点 S_i 到目标节点的数据传输要经过 k 跳，那么定位数据传输所消耗的总能耗为：

$$E_T=2E'+E''D^n_{ij}+\sum_{i,j=1}^{n}(2E'+E''D^n_{ij}) \tag{5}$$

在光纤网络链路中布置继节点的关键是基于源节点、目标节点之间的距离以及损坏关系来选择最佳的放置位置[13]。光纤网络中的协作通信是源节点集合 $S=\{s_1,s_2,\cdots\cdots,s_n\}$，将数据通信信息通过中继节点传送到目标节点集合 $Q=\{q_1,q_2,\cdots\cdots,q_m\}$。本文仅考虑 $m=1$ 的情况，此时接收的通信信号具有一致性，接收端接收到的信号 $r(t)$ 为：

$$r(t)=\sum_{i=1}^{n}|w_i|\varphi(t)+\eta(t) \tag{6}$$

其中，$\sum\limits_{i=1}^{n}|w_i|\varphi(t)$ 为接收功率的总和，$\eta(t)$ 为初始信号。

光纤网络在被入侵后，理论上选取节点在其传输半径内的其它节点都可以接收到数据信息。在计算出能耗的基础上，设计阈值，部署中继节点进行协作通信能够减少选取死亡节点的可能，改善入侵后网络通信带宽，提高链路性能。其入侵后中继节点选取示意图如图 2 所示。

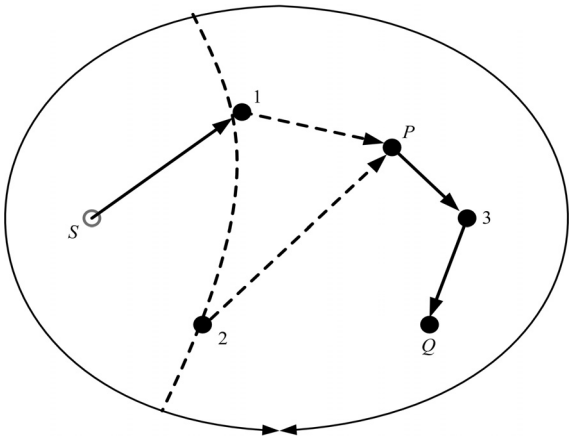

图 2 入侵后中继节点选取示意图

当源节点 S 发送传输数据到目标节点 Q 时，连接路径是 $S\rightarrow1\rightarrow P\rightarrow3\rightarrow Q$，节点 S 发送节点 1 时，此时节点 2 也可以接收到数据；当网络被入侵后，经过中继节点 P 也可以最终将数据传输到目标节点 Q，通过对最优数量的中继节点的部署，使整个光纤网络可完成通信，提高了网络的覆盖率和安全性。

3 实验结果与分析

3.1 实验环境

设定光纤网络仿真监测区域的面积大小为 300m×200m，光纤传感器源节点坐标为(300,10)、通信半径 r_1 为 50m，布置的中继节点通信半径 r_2 为 100m。中继节点通信容量上限为 50bit。光纤网络中部署的中继节点的数目为 20 个，节点坐标由 Matlab 随机函数产生，光纤网络传感器节点的数据流量随机分配，如表 1 所示。

表 1 中继节点的坐标及数据量

节点标号	坐标	数据量	节点标号	坐标	数据量
1	175,4.02	5	11	135,0.45	7
2	183,3.65	8	12	69,4.56	8
3	115,2.36	7	13	23,3.06	7
4	126,4.75	9	14	75,2.54	9
5	85,2.05	3	15	241,2.15	4
6	140,0.86	4	16	148,3.25	6
7	89,1.84	7	17	78,1.24	4
8	49,3.05	5	18	65,2.50	3
9	79,4.36	6	19	245,1.54	4
10	134,2.74	9	20	154,0.98	8

3.2 开销对比

本文的选取算法和传统 BP 算法的开销情况如图 3 所示，在不同的中继节点数量情况下，本文算法(移动中继节点动态分布选取算法)的通信开销远远小于传统 BP 算法的通信开销。

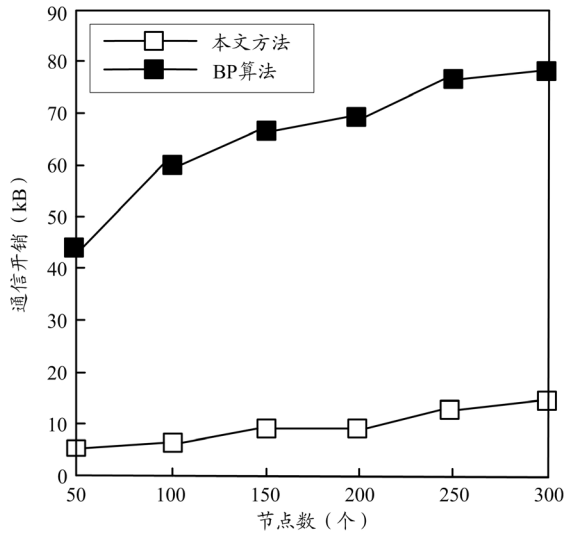

图 3 不同方法下通信方面开销对比

3.3 算法复杂度对比

复杂度是评价算法优良性的一个重要指标，为了测试本文算法的有效性，将 BP 算法与本文算法作对比，其算法复杂度测试结果如表 2 所示。

表 2 不同方法复杂度测试结果

准确率(%)	本文算法执行次数	BP 算法执行次数
95	2583	4890
90	2007	4293
80	1349	3893
70	987	3453
60	845	3098
50	728	287

由表 2 可以看出，当达到相同的选取准确率，本文算法执行的次数明显低于 BP 算法的执行次数，说明本文算法的复杂度低于 BP 算法的复杂度，可见本文算法优于传统的 BP 算法，具有更高的选用价值。

3.4 算法误差对比

平均选取误差是用来评价入侵移动中继节点动态分布选取的指标，本文分别采用两种算法对入侵移动中继节点动态分布选取，并记录入侵移动中继节点动态分布选取耗时，数据对比如表 3 所示，两种算法的平均误差趋势如图 4 所示。

由表 3 和图 4 可以看出，采用本文算法不仅对入

表 3 两种算法选取耗时

算法类别	选取耗时(s)	平均误差水平(%)
BP 算法	13.5	2.2
本文算法	5.2	0.5

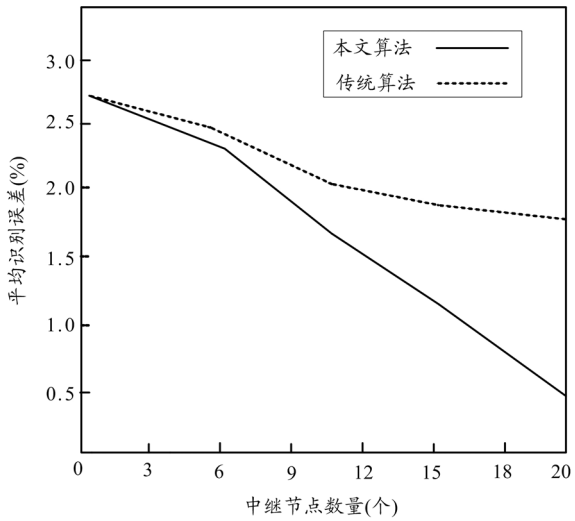

图 4 平均识别误差对比

侵移动中继节点动态分布选取耗时少,而且选取平均误差小,两者指标都明显低于 BP 算法,说明本文算法具有很强的应用性。

3.5 选取算法整体性能评价

对算法的整体性能进行分析，根据本文算法、BP 算法的性能,绘出相应的虚警率(ROC)曲线,如图 5 所示。

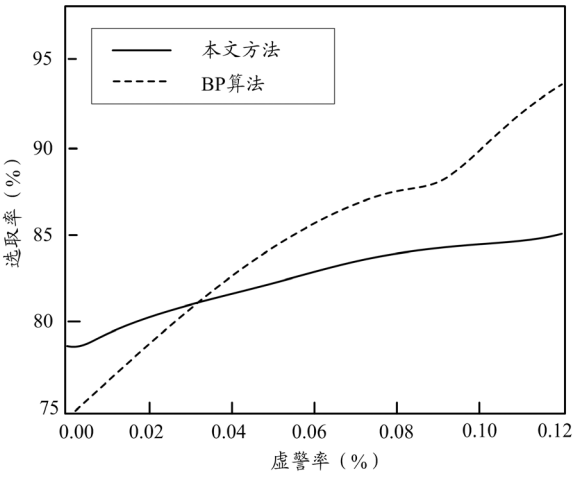

图 5 两种算法 ROC 曲线比较结果

对图 5 进行分析可知，只在一少部分区域 ROC 下，本文算法的 ROC 曲线大部分区域高于 BP 算法，且 ROC 曲线浮动值也是最平稳的,表明本文算法具有较好的整体检测性能。

4 结束语

本文提出了光纤网络在恶意数据入侵下移动中继节点动态分布选取算法,考虑了在入侵环境下设计合理的节点选择算法,以此提高光纤网络在入侵下的网络覆盖率和链路性能。实验证明,我们提出的算法在网络均衡负载和恶意数据入侵识别误差方面具有较好的有效性和可靠性。但是,在强干扰环境下,算法的鲁棒性不强,运行成本较大,这是需要下一步继续解决的问题。

参考文献:

[1] 裴丽,翁思俊,吴良英,等. 光纤激光传感系统的研究进展[J]. 中国激光, 2016(7):1–7.

[2] 蒋清健, 张文超. 无线传感器网络的节点自适应定位算法研究[J]. 应用激光, 2015(6):729–732.

[3] SHAHZAD M K, CHO T H. Extending the network lifetime by pre-deterministic key distribution in CCEF in wireless sensor networks[J]. Wireless Networks, 2015, 22(8): 1–11.

[4] NGUYEN L V, KODAGODA S, RANASINGHE R, et al. Information-Driven adaptive sampling strategy for mobile robotic wireless sensor network [J]. IEEE Transactions on Control Systems Technology, 2015, 24 (1):1–1.

[5] 梁頔,马铁华. 光纤与测试节点的星型拓扑测试网络构建方法[J]. 中北大学学报(自然科学版), 2015,45(5):592–596.

[6] 张引发,任帅,廖晓闽,等.光网络中大功率带间串扰攻击研究[J]. 激光与光电子学进展, 2014, 51(8):65–71.

[7] NORDIO A, TARABLE A, DABBENE F, et al. Sensor selection and precoding strategies for wireless sensor networks [J]. IEEE Transactions on Signal Processing, 2015, 63(16): 4411–4421.

[8] MOHAMADI H, SALLEH S, ISMAIL A S, et al. Scheduling algorithms for extending directional sensor network lifetime [J]. Wireless Networks, 2015, 21(2): 611–623.

[9] 寇媛媛. 光纤激光网络中的被入侵节点定位方法研究 [J]. 西安职业技术学院学报, 2016,23(12):141–145.

[10] BOZKURT A, LOBATON E, SICHITIU M. A biobotic distributed sensor network for under-Rubble search and rescue[J]. Computer, 2016, 49 (5): 38–46.

[11] LIN H Y. Location-based data encryption for wireless sensor network using dynamic keys[J]. Wireless Networks, 2015, 21(8): 1–8.

[12] 王翥,吕翠翠,王玲. 无线传感器网络中继节点的布局算法[J]. 仪表技术与传感器, 2014(1):85–88.

[13] 陈二虎, 刘颖, 刘璐, 等. 激光链路中继卫星系统网络设计及性能分析[J]. 红外与激光工程, 2015,44(9):2778–2782.