一种恶意节点攻击的无线传感器网络入侵检测方法

董 峰,张秋霞
(黄河科技学院 现代教育技术中心,河南 郑州 450063)

摘 要:无线传感器节点通常被随机部署在没有基础网络设施的场所,当传感器节点位置暴露在恶意攻击环境时,攻击者会攻击网络覆盖漏洞,节点易受到未知攻击从而导致定位错误,无线传感器网络很难在没有人工参与的情况下安全运行。针对此问题,设计了一种基于无线传感器网络节点的入侵检测算法。该算法能解决无法识别的未知攻击问题,通过聚类技术检测攻击产生的异常值,并在理论上证明了该算法的正确性。通过测试和实验手段,验证了该算法在保护传感器网络的前提下,完成了对未知攻击的检测、修复和定位。

关键词:无线传感器;聚类算法;移动节点;检测
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2017)02-0086-04
doi:10.3969/j.issn.1673-629X.2017.02.020

An Intrusion Detection Method for Wireless Sensor Network of Malicious Node Attack

DONG Feng, ZHANG Qiu-xia
(Modern Education Technology Center, Huanghe Science and Technology College, Zhengzhou 450063, China)

Abstract: Wireless sensor nodes are usually random deployment in the absence of infrastructure network. When the sensor node position exposed to malicious attacks environment, the attacker will attack the network coverage holes, and nodes are vulnerable to unknown attacks leading to positioning error. Wireless sensor networks is difficult to operate safely in no case of human involvement. To solve this problem, an intrusion detection algorithm based on wireless sensor network node is designed, which can solve the problem of unrecognized unknown attacks. The outliers generated by attacks are detected through clustering techniques, and the correctness of the algorithm is proved theoretically. Test and experiment means that the algorithm on the premise of protecting the sensor network completes the unknown attack detection, repair and positioning.

Key words: wireless sensor; clustering algorithm; mobile node; detection

0 引 言

无线传感器网络(Wireless Sensor Networks, WSN)应用于安全反恐、环境检测、智能交通及目标追踪等领域中,其移动节点安全程度是传感器网络服务质量的重要标准[1]。

移动节点定位技术是无线传感器网络服务的基础,当前异常检测解决方法主要通过寻找测量值的偏差来捕捉已知的攻击属性参数[2-3]。无线传感器网络在入侵检测方面的研究已有一些成果。Krontiris 等对有限次攻击的异常行为进行了侦测研究,通过节点在网络中的均匀分布减少节点安全漏洞[4]。为了检测未知的异常攻击,叶苗等提出了一种新的容忍恶意节点攻击的无线传感器网络安全定位方法,通过变方差特征的传感器节点定位概率模型提高传感器网络的灵活性和适应性[5]。Kaplantzis 基于商业化角度研究了异常故障中模糊和嘈杂的信息,通过节点移动来实现避开障碍物的集中式算法,提高了传感器网络的安全性和完整性[6]。

现有研究实现的功能主要是依据已知的攻击或检测到的节点变化参数[7-8]。文中采用集群技术来检测移动节点在时间和空间上的不同特征,在检测到移动节点的异常因素后,能将受隐蔽的攻击者影响的移动

收稿日期:2015-11-24 **修回日期**:2016-03-17 **网络出版时间**:2017-01-10
基金项目:2014年度河南省科技攻关项目(142102210641);2015年度河南省高等学校重点科研项目(15A520085)
作者简介:董 峰(1972-),男,副教授,研究方向为计算机网络。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20170110.0941.002.html

节点孤立于网络。

1　基本假设

为方便无线传感器网络的描述和讨论,做如下攻击假设:

(1)移动节点在无线传感器网络中受到了保护,无线传感器网络协议中聚合、路由与时间同步,移动节点能够表现出有偏差的聚合值,包括错误的检测值或遭受损坏的聚合节点。

(2)攻击目标包括静态节点和移动节点,所体现的攻击信息主要指信息感知系统提供的错误图片。

(3)攻击者攻击节点造成响应时延或失去各个节点的同步时钟信号,接收到的关键信息不是最新信息,造成无线传感器网络不稳定。

(4)路由协议遭到攻击后路径发生改变,数据不能准确到达接收器或产生一个较大的延迟,这种攻击恶意改变了节点在路由表中存储的数据值。

(5)攻击者客观上恶意篡改数据,呈现出虚假的数据。

2　受损节点特征提取模型

假定移动节点在不同时间段内的频率不同,通过空间上遥感数据不一致问题来检测操控数据和遭到损害的节点。提取模型如下:

(1)假设无线传感器网络的移动节点在数据输出窗口中显示的 n -程序尺寸比例为20:11110000001111110000,用户提取所有序列大小为3(固定尺寸为3),向量每次向前移动一个位置。

(2)在所显示的时间段窗口中,111发生6次,110发生2次,000发生6次,001发生1次,011发生1次。所提取的矢量对应的时间窗口显示:111-0.33,110-0.11,100-0.11,000-0.33,001-0.06,0.11-0.06。

(3)在受损节点特征提取模型中,序列的特征值和它们的频率特征值相对应,所有特征值的总和为1,所提出的算法向量在预定义的时间段内每行提取40个特征值。

利用上述模型特征,在节点上形成空间模型,节点附近搭建控制台。在某一时刻的时间内,n -程序空间表征每隔一个时间段从传感器中输出数据。同一组传感器 S_1,S_2,S_3 在1110四个时间段内输出,依据 n -程序部署(每个 n -程序按照 S_1 值第一位置,S_2 值第二位置,S_3 值第三位置),传感器在一个时间段内发生的频率:111三次,000一次。产生 n -程序的特征值是:111-0.75,000-0.25。接收器显示的节点接收路径数据:A-B-C-S三次,A-D-E-F-S两次,A-B-E-F-S一次(A指节点发送数据,B、C指网络中其他节点,S指接收器),对应的 n -程序(n =3):ABC,BCS,ADE,DEF,EFS,ABE和BEF。路由器端口显示,n -程序中ABC产生3次,BCX产生3次,ADE产生2次,DEF产生2次,EFS产生3次,ABE产生1次,BEF产生1次,n -程序的总数量为15。

3　修复未知攻击节点策略

3.1　未知攻击的覆盖范围评价指标

文中修复集群攻击技术采用SOM神经网络[9]、遗传算法(GA)[10]和生长型神经气算法[11]。接收器窗口显示的数据包括被攻击和未被攻击的数据,通过算法优化减少传感器网络节点遭受攻击产生的时间滞后问题。以MD表示集群之间的平均距离,以QE表示计算量化误差,检测节点遭受攻击的路径公式如下:

$$\sum_{i=0}^{n}\Delta f_i = 0 \tag{1}$$

其中,n 为 n -程序变化的特征值。

$$\Delta D = \sum_{i=1}^{N}|\Delta f_i| \tag{2}$$

上述公式计算QE和MD值的变化,用 f_{th} 表示正常情况下的攻击,遭受攻击后的变化如下:

$$\sum_{i=1}^{N}|\Delta f_i| > f_{th} \tag{3}$$

当 ΔD 的值接近0时,该值不影响 n -程序中描述的变化,得出:

$$D_{max} = 2n * f_{err} = \frac{2nN_{err}}{N_{sample}} \tag{4}$$

模拟 n -程序从0到 D_{max} 的变化:

$$F(\rho) = \beta + (1-\beta)e^{\kappa\alpha} \tag{5}$$

其中,$\alpha = 1 - \frac{1}{\rho}$;$\beta < 1$;$\kappa$ 为常量系数;ρ 为 n -程序系数。

给出一组随机变量 $x_1, x_2, \cdots, x_k$,得出如下公式:

$$C(x_1, x_2, \cdots, x_k) = \sum_{i=1}^{k}H(x_i) - H(x_1, x_2, \cdots, x_k) \tag{6}$$

当 $H(x_i)$ 随 x_i 的信息发生变化,依据 $x_1, x_2, \cdots, x_k$ 的值得出 $H(x_1, x_2, \cdots, x_k)$ 的值。

β 的设置使得 $F(\rho)=1$,当 $\kappa \to 0$,功能接近相同的渐近函数,当 $\kappa \to \infty$,功能达到渐近线 $F(\rho)=0$。如果 $\rho < 1$,$F(\rho)=1$;$\rho = 1$,得出:

$$F(\rho)\frac{2nN_{err}}{N_{sample}} > f_{th} \tag{7}$$

检测到的最小攻击数为:

$$N_{errmin} = \frac{N_{sample}}{2nF(\rho)}f_{th} \tag{8}$$

如果 β 值增加或者 κ 值减少,N 的值将减少;反

之，ρ 值减小或者 κ 值增加，N_{sample} 将趋向于 N_{errmin}，结果如下：

$$\beta > \frac{N_{sample}}{2nN_{errmin}} f_{th} \tag{9}$$

3.2 分布式探测器设计

基于无线传感器网络的分布式特征，使用探测器分布式技术实现软件代理和所在的物理节点。计算移动节点对于 SOM 网络的移动方格，基于 GA 的交叉和变异概率，得出最优参数。使用代理冗余的方式实现物理节点的分配，对每个节点周围配置信息接收代理，对所有节点信息计算加权和。统计理论为：

$$R = E(\text{Bate}(\alpha + 1, \beta + 1)) = \frac{\alpha + 1}{\alpha + \beta + 1} \tag{10}$$

其中，α 表示检测器的数量；β 表示错误的数量，传感器系统能反映出正确或错误的物理节点。

移动节点在运转时为了减少周边干预，在节点遇到其他节点信号干扰时，分两种情况判断：其一是节点仍在同一区域，位置没有发生显著的变化，仍接收集群节点中的路由数据；其二是已经改变了位置，接收到的数据发生了明显的变化，节点的路径发生了改变。

3.3 受损节点的隔离和修复

对测试的传感器网络中每个节点模拟算法攻击，遭受攻击后的节点检测到异常行为后，检测丢失的数据或请求其他路由器节点响应，及时将受损节点从无线传感器网络隔离后重组，保护其他节点的性能，避免影响下一个路由器的运转。

遭受攻击后的节点形成新的 n-gralm，假设能够准确从攻击者发出矢量中提取子集，通过提取 repQE 和 repMD 的值，得出两个函数值。

```
if(QE<1)
{repQE=1;}
else
{repQE=1-QE/2;}
if(MD<1)
{repMD=1;}
else
{repMD=1-MD/2;}
if(QE>1)
{rep=repQE;}
else
{rep=repMD;}
```

这两个函数能区分节点正常或异常行为，如果当前的矢量特征值高于节点的最高值则可能有攻击现象，如果与节点正常显示值相符，节点将正常运行。

```
if(last_rep[node]>threshold)
{new_rep[node]=last_rep[node]+rep+log(1.2*rep);}
else
{new_rep[node]=last_rep[node]+c_limit+log(1.2*rep);
```

系数 c 低于 1 时，last_rep[node]值将位于[0,1]区间，当 c 大于 1 时，last_rep[node]将取中间值。即使在测试时间内相互干扰，使用聚类算法将得到比较高的准确值。

```
if(value_rep<threshold)
{if(space_rep <threshold)
{result=value_rep;}
else{result=1-value_rep;}}
else
{result=value_rep;}
```

矢量特征不一致时发生的异常现象容易被检测到，当路由协议发生异常时，将出现某个遭到破坏节点的路由路径，从而在节点源查找攻击原因。如果路由器没有发生异常现象，将出现正确路线 nGood，相反将出现遭破坏的数值：$\frac{\text{nGood}}{\text{nGood} + \text{nBad}}$，通过这种方式不良节点的破坏行为将大幅减少。

4 检测结果分析

通过模拟器验证算法对抗未知攻击的准确性，模拟器能不依赖于传感器实现节点通信功能，方便传输其他传感器的数据。模拟器划分为多个集群，其中每个组都有簇头，簇头参与不同集群之间的通信。传感器节点随机移动，节点移动的最长距离不超过当前位置和目标距离的 20%。

4.1 模拟未知攻击

将受到未知攻击的节点上配置多个 ID，并发送随机值，把 40 个通过模拟器测试的节点随机放置在 100 个不同的位置，模拟对传感器网络检测节点恶意攻击，持续时间为 1 000 个刻度，接近传感器的节点在相同时间段内输出的结果放置到同一组，模拟器在一个时间刻度内的采样周期如图 1 所示。

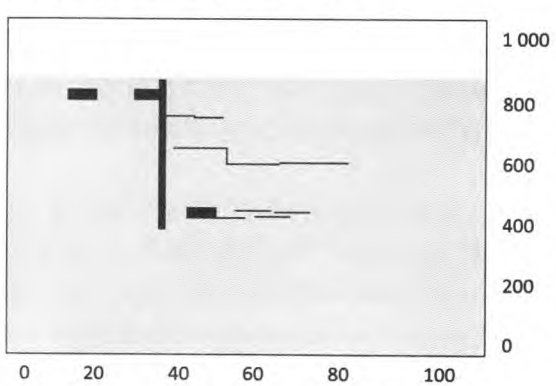

图 1 顶层视图—2D

4.2 算法模拟分析

搭建实验平台，在第一个实验中检测静态节点（在位置 26 处实施攻击），可以从不同角度观察到检测节点在第 26 位移动节点受损程度明显降低，如图 2

所示。在第二个实验中采用密闭攻击动态节点的方式,通过顶层视图划分受感染的移动节点。结果表明降低了节点受攻击概率。

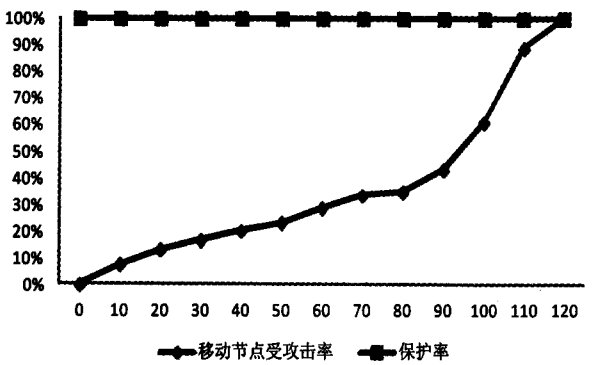

图2　恶意节点的平均检测率

根据图2显示的结果,如果检测节点发出的攻击80%是恶意的,文中所提出的算法可以完全检测到攻击,差错率为0%。

图3验证了如何检测和完全隔离的攻击时间以及恶意网络中节点的总数。

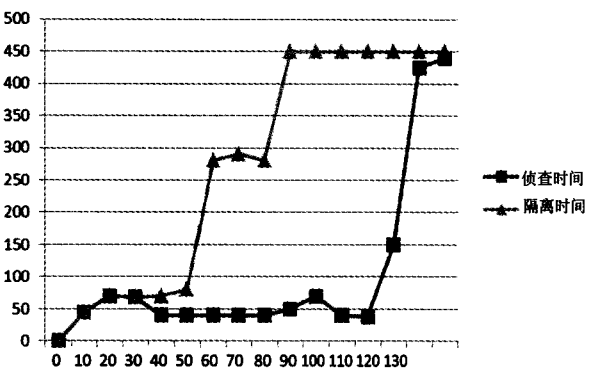

图3　侦查和隔离时间

5　结束语

因为多方面的原因,无线传感器网络节点容易受到未知攻击,及时发现并修复攻击是提高网络可靠性的重要方法[12]。提出了一种检测无线传感器网络未知攻击的算法,并设计了受损节点的修复方案,仿真实验证明了该算法的正确性。在含有移动节点的无线传感器网络中,算法能够检测到节点周围的未知攻击,并能全部检测出恶意攻击的节点数,对受损节点进行有效隔离,实现了更合理的节点部署。

参考文献:

[1] 赵忠华,皇甫伟,孙利民,等. 无线传感器网络管理技术[J]. 计算机科学,2011,38(1):8-14.

[2] Hai T H, Khan F I, Huh E. Hybrid intrusion detection system for wireless sensor networks[C]//Proceedings of international conference on computer science and applications. San Francisco, CA, USA: [s. n.], 2007.

[3] Loo C E, Ng M Y, Leckie C, et al. Intrusion detection for routing attacks in sensor networks[J]. International Journal of Distributed Sensor Networks, 2006, 2(4): 313-332.

[4] Krontiris I, Giannetsos T, Dimitriou T. LIDeA: a distributed lightweight intrusion detection architecture for sensor networks[C]//Proceedings of the 4th international conference on security and privacy for communication networks. Istanbul, Turkey: [s. n.], 2008.

[5] 叶　苗,王字平. 一种新的容忍恶意节点攻击的无线传感器网络安全定位方法[J]. 计算机学报,2013,36(3):532-545.

[6] Kaplantzis S, Shilton A, Mani N, et al. Detecting selective forwarding attacks in WSNS using support vector machines[C]//Proceedings of 3rd international conference on intelligent sensors, sensor networks and information. Melbourne, Australia: [s. n.], 2007: 335-340.

[7] Adaptive Security Analyzer[EB/OL]. 2012-02-27. http://www.privacyware.com/index_ASAPro.html.

[8] Bankovi ć Z, Fraga D, Moya J M, et al. Bio-inspired enhancement of reputation systems for intelligent environments[J]. Information Sciences: An International Journal, 2013, 222: 99-112.

[9] Bankovi ć Z, Moya J M, Araujo A, et al. Distributed intrusion detection system for wireless sensor networks based on a reputation system coupled with kernel self-organizing maps[J]. Integrated Computer Aided Engineering, 2010, 17(2): 87-102.

[10] Wagfer D. Resilient aggregation in sensor networks[C]//Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks. [s. l.]: ACM, 2004: 78-87.

[11] 罗永健,史德阳,侯银涛,等. 基于相似度的无线传感器网络数据复原汇聚方法[J]. 计算机应用研究,2012,29(9):3405-3407.

[12] 王　珊,王庆生,樊茂森. 基于移动节点的无线传感器网络覆盖空洞修复方法[J]. 传感器与微系统,2015,34(4):134-136.