doi: 10.3969/j.issn.1006-1576.2012.01.014

一种有效的无线传感器网络攻击检测方法

罗永健，史德阳，于茜，张卫东
（西安通信学院，西安 710106）

摘要：针对现有无线传感器网络攻击检测算法检测率低、计算复杂度高等问题，提出一种新的基于分簇模型的无线传感器网络攻击检测算法。借鉴集中式数据汇聚模型中二分比较法的思想，对分簇式无线传感器网络中各簇均值进行二分比较，利用两部分均值的残差的统计特性进行攻击检测，并在相同实验条件下对二分比较法和 t 检验法进行对比分析。仿真结果证明，该算法的攻击检测性能要优于现有的攻击检测算法。

关键词：无线传感器网络；数据汇聚；攻击检测
中图分类号：TP393.06　　**文献标志码**：A

An Effective Attack Detection Algorithm in Wireless Sensor Networks

Luo Yongjian, Shi Deyang, Yu Qian, Zhang Weidong
(*Xi'an Communications Institute, Xi'an* 710106, *China*)

Abstract: For the low attack detection rate and high computational complexity of the existing attack detection algorithm in wireless sensor networks, a new attack detection method based on clustering is proposed. The method uses the idea of sample halving, by which the halved two parts of the cluster averages are checked against each other. Under the same experimental conditions, the new algorithm is compared with the sample halving and the t-test method. Simulation results show that the performance of the new algorithm is better than the existing attack detection algorithm.

Key words: wireless sensor networks; data aggregation; attack detection

0　引言

数据汇聚是无线传感器网络(wireless sensor networks，WSN)中减少数据传输量、消除数据冗余、降低网络能耗、延长网络寿命的一项关键技术，但受 WSN 节点部署环境和通信信道的影响，数据汇聚在安全问题上面临着严峻挑战[1]。特别是当攻击者俘获 WSN 中的部分节点并篡改其读数时，常规的加密和认证措施都将失效，汇聚误差将保留在最终的汇聚结果中，进而影响用户的决策。因此，在进行数据汇聚处理前对汇聚函数的输入值(即传感器节点感知的源数据)进行攻击检测是十分必要的。

目前相关学者针对 WSN 攻击检测算法已开展了广泛研究：Buttyan 提出一种针对数据复原汇聚的二分比较攻击检测法[2]，该算法建立在集中式数据汇聚模型基础上，能耗较大且攻击检测率低；文献[3]提出一种基于分簇模型的卡方检验攻击检测算法，在能耗和检测性能方面较二分比较法有明显改善，但该算法对均匀分簇和非均匀分簇的检测算法不同，计算复杂度较高且攻击检测能力仍然较低；Qinren Shu 提出一种基于密集数据挖掘的数据复原汇聚算法[4]，采用信息挖掘技术，对恶意攻击有较高的抵抗能力，但在 WSN 中不存在攻击时该算法仍会剔除边缘数据，影响汇聚精度；为了克服上述不足，文献[5]提出一种基于 t 分布的无线传感器网络攻击检测法，该算法检测率较高，并且放宽了对感知数据先验知识的要求，但其攻击检测效果与参考簇的选取有关，当参考簇选为不受攻击或攻击较弱的簇时检测效果不太理想。针对以上算法存在的不足，笔者借鉴集中式数据汇聚模型中二分比较法[2]的思想，提出了一种新的基于分簇模型的无线传感器网络攻击检测算法。

1　攻击检测模型

分簇模型利用分簇算法将 WSN 划分为若干个簇，每个簇含有若干个传感器节点，选择其中一个节点充当簇头。簇头对所在簇的节点的感知数据进行汇聚处理，将汇聚结果通过单跳或多跳路由传送至基站，基站对收集到的数据利用攻击检测算法进行攻击检测。新算法的攻击检测模型假设如下：

1) $k \le 0.5$，其中 k 是受攻击节点占所有传感器节点的比例。攻击者不能在网络中随意选择节点进行攻击，否则所有的攻击检测算法都将失去作用。

收稿日期：2011-08-01；**修回日期**：2011-09-05
基金项目：国家自然科学基金资助项目(61179002)；陕西省自然科学基础研究计划资助项目(2011JM8030)
作者简介：罗永健(1971—)，男，湖北人，博士，教授，从事阵列信号处理、雷达目标识别及多用户通信等研究。

2) 节点攻击方式为加性攻击。加性攻击有增量攻击和常量攻击 2 种。对每个被俘获节点读数都增加一个相同值即为增量攻击，修改被俘获节点读数使其达到同一个值即为常量攻击。

3) 被俘获节点分布相对集中。攻击者往往在操作方便的范围内选择节点进行攻击，故假设被俘获节点相对集中于网络的某个或某些簇是合理的。

2　新算法的基本原理

为了表述方便，特定义以下符号：n 为 WSN 中节点的总数目；r 为 WSN 中分簇的数目，为方便起见，笔者假定 r 为偶数；C_i 为 WSN 的第 i 个簇；m_i 为簇 C_i 中所含节点的数目；X_{ij} 为簇 C_i 中第 j 个节点的读数；$\overline{X_i}$ 为簇 C_i 中所有节点读数的平均值；α 为显著性水平；k 为受攻击节点占所有节点的比例；K 为受攻击节点数目；add 为攻击增量。

假定未遭受攻击的传感器节点读数服从独立同分布，且期望 μ 未知，方差 σ^2 已知。根据中心极限定律，簇 C_i 中各传感器读数之和 Y_i 服从高斯分布，即

$$Y_i=\sum_{j=1}^{m_i}X_{ij}\sim N(m_i\mu,m_i\sigma^2),\ (i=1,2,\cdots,r) \tag{1}$$

则簇 C_i 中样本数据的平均值 $\overline{X_i}$ 服从分布

$$\overline{X}_i=\frac{1}{m_i}\sum_{j=1}^{m_i}X_{ij}\sim N(\mu,\frac{\sigma^2}{m_i}),\ (i=1,2,\cdots,r) \tag{2}$$

常用的聚合函数有求均值、最大值、最小值等，笔者只考虑求均值的情况。各簇中传感器节点将自身感知的数据无线传输到簇头节点，簇头节点对接收到的数据进行汇聚处理，只需将各簇均值 $\overline{X_i}$ 传递给基站，故大大减少了数据传输量，节约了传感器节点的能耗。

基站接收到各个簇的均值 $\overline{X_i}$ 后，将其等分为 2 部分 W_1 和 W_2，2 部分的残差为 W。由于 $\overline{X}_1$，$\overline{X}_2$，…，$\overline{X}_r$ 两两之间相互独立，故 W_1 和 W_2 相互独立，由概率论和数理统计的知识可得 W_1 和 W_2 和 W 服从以下分布

$$W_1=\sum_{i=1}^{r/2}\overline{X_i}\sim N(\frac{r}{2}\mu,\sigma^2\sum_{i=1}^{r/2}\frac{1}{m_i}) \tag{3}$$

$$W_2=\sum_{i=\frac{r}{2}+1}^{r}\overline{X_i}\sim N(\frac{r}{2}\mu,\sigma^2\sum_{i=\frac{r}{2}+1}^{r}\frac{1}{m_i}) \tag{4}$$

$$W=W_1-W_2\sim N(0,\sigma^2\sum_{i=1}^{r}\frac{1}{m_i}) \tag{5}$$

当 WSN 中不存在攻击时，残差 W 将服从期望为零的正态分布，否则残差 W 将不再严格服从正态分布。因此，可根据残差 W 的统计特性，将 W 与一个门限值 h_α 进行比较，以判断网络中是否存在攻击行为，即

$$D(\overline{X}')=\begin{cases}1 & if\ |W|>h_\alpha\\ 0 & otherwise\end{cases} \tag{6}$$

式中：$\overline{X}'$ 为基站接收到的样本数据；$D(\overline{X}')$ 是攻击判断函数，当网络中不存在攻击时结果为 0，否则其结果为 1。

门限值 h_α 由系统给定的检测虚警率求得，即

$$\Pr\{|W|>h_\alpha|H_0\}=2-2\Phi\left(h_\alpha\Big/(\sigma\sqrt{\sum_{i=1}^{r}\frac{1}{m_i}})\right)=\alpha \tag{7}$$

式中：H_0 表示攻击不存在的假设；α 为显著性水平，在文中含义为虚警率。

当有 K 个节点遭受到攻击时，攻击者对数据汇聚结果所造成的偏差为

$$d=\frac{K\,add}{n} \tag{8}$$

从式 (5)、(6)、(7) 可以看出，与 t 检验法[5]相比，新算法计算量较小且复杂度较低。新算法对均匀分簇和非均匀分簇的攻击检测公式一样，普适性强，而卡方检验法[3]则需分别针对均匀分簇和非均匀分簇进行讨论，计算复杂度较高。新算法的攻击检测率难以用公显式表示出来，实际应用中可通过蒙特卡罗方法求得近似的检测率。

3　性能仿真

将 100 个传感器节点随机部署在 100 m×100 m 的区域内，假定在 WSN 中不存在攻击时，传感器节点的感知数据服从方差为 1 的高斯分布，显著性水平 $\alpha=0.05$。笔者针对无线传感器网络非均匀分簇和均匀分簇 2 种情形对新算法进行 Matlab 实验仿真，并在相同实验条件下与二分比较法[2]和 t 检验法[5]进行了对比分析。仿真图中纵坐标为攻击检测率，单位为 1；横坐标为偏差，单位以实际应用中传感器所测参数为准。针对不同的受攻击节点数目 k，计算机仿真中均进行 200 次的蒙特卡罗实验。

3.1　非均匀分簇时新算法的性能仿真

将无线传感器网络划分为节点数各不相等的 6 个簇，各簇节点数分别为 5、8、15、20、24 和 28，代入式 (7) 中并查表可求出门限值 h_a=1.368 9。图 1～图 4 分别为 K=1、K=2、K=2 和 K=35 时新算法与二分比较法和 t 检验法的仿真结果对比。

如图 1，当 K=1 且参考簇为受攻击簇时，t 检验法的检测效果较为理想，而当参考簇为不受攻击簇时的检测效果极差，这是因为只有一个节点遭到攻击时，各簇的均值与不受攻击簇的均值的差异之和很小，故检测率很低。而新算法则弥补了了 t 检验法这一缺陷。由图 2 和图 3 可知，二分比较法的攻击检测率在 K=2 和 K=2 时无法收敛于 1。仿真实验表明，当攻击节点数为偶数时，二分比较法的攻击检测率都无法收敛于 1，因为若等分的两部分数据所包含的受攻击节点数目相等，两部分数据的残差之和将为零。新算法虽然借鉴了二分比较法的思想，却不存在这种问题。

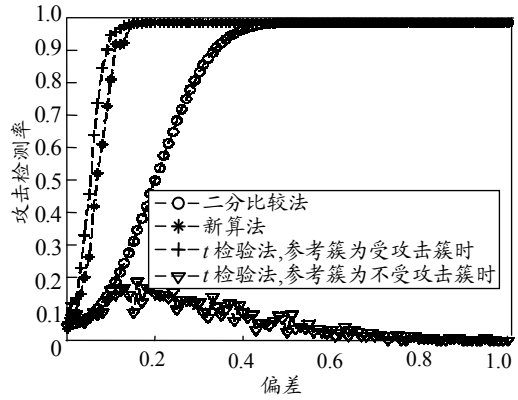

图 1　K=1 时检测率的比较

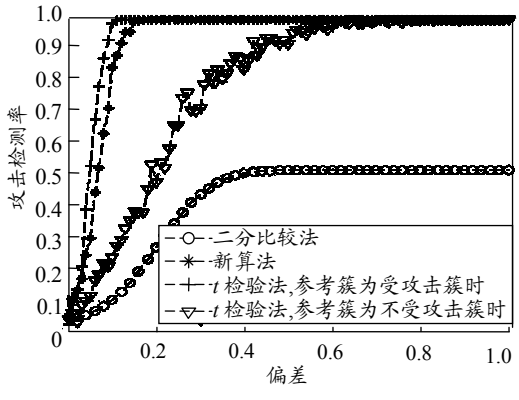

图 2　K=2 时检测率的比较

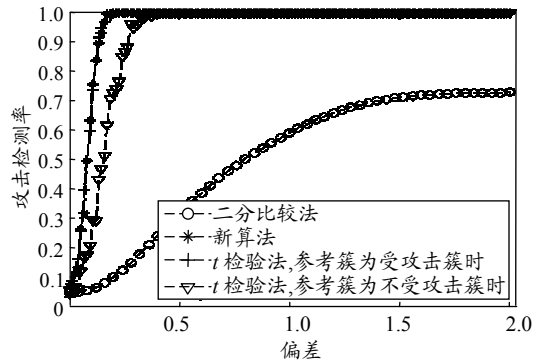

图 3　K=8 时检测率的比较

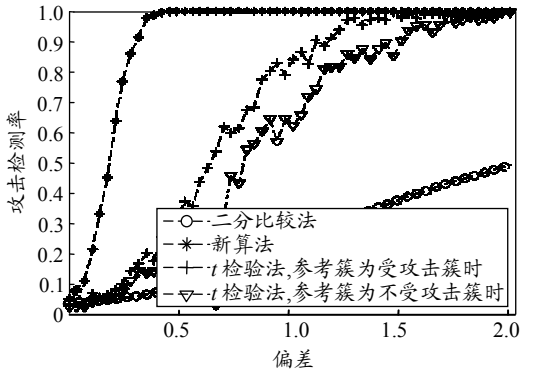

图 4　K=35 时检测率的比较

对比图 1～图 4 可得，当 t 检验法的参考簇为不受攻击簇时，新算法的检测率较高；当 t 检验法的参考簇为受攻击簇时，K=8时新算法和 t 检验法的检测率相当，K<8时 t 检验法的检测效果好于新算法，K>8时新算法的检测率要高于 t 检验法。实际应用中，攻击者为了增加汇聚误差，往往选择较多的节点进行攻击，此时新算法有更好的检测性能。

3.2　均匀分簇时新算法的性能仿真

将无线传感器网络均匀划分为 10 个簇，各簇节点数均为 10，代入式 (7) 中并查表可求出门限值 h_α=1.9。图 5～图 7 分别为 K=3、K=25 和 K=35 时的仿真结果。

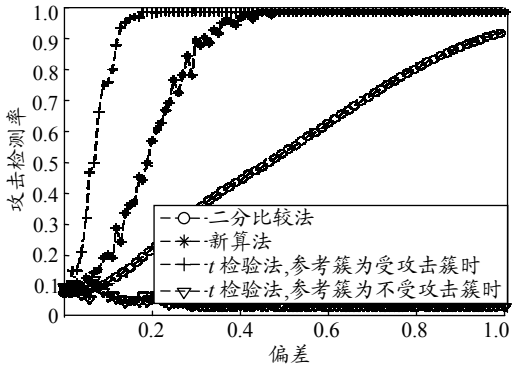

图 5　K=3 时检测率的比较

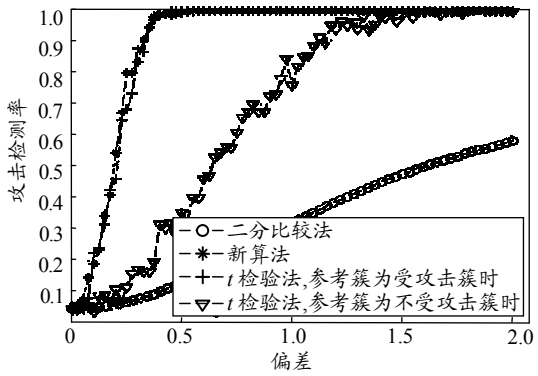

图 6　K=25 时检测率的比较

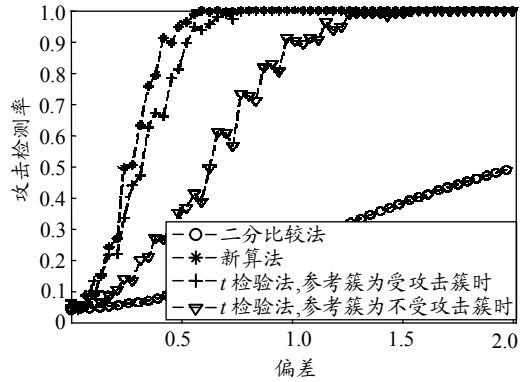

图 7　K=35 时检测率的比较

由图 5 可知，在 $K=3$ 且参考簇选为受攻击的簇时，t 检验法的攻击检测率高于新算法，这是因为新算法考虑的是两部分均值的残差，而 t 检验法则综合考虑了组内偏差平方和及各簇均值的差异。当 K 较小时，对各簇的攻击均未达到饱和，受组内偏差平方和的影响，t 检验法的攻击检测率较高；当 K 较大时，网络中某一簇或某些簇的攻击达到饱和，此时组内偏差平方和达到最大值。当被俘获的节点数继续增加，组内偏差平方和的值将逐渐减小，所以 t 检验法的攻击检测率就会逐渐降低，但受簇间均值差异的综合影响，其攻击检测率仍然增大。而新算法考虑的是两部分均值的残差，当攻击节点数较多且较为集中时，残差的值则越大，攻击检测率也越高。

对比图 5、6、7 知，当 t 检验法的参考簇选为不受攻击的簇时，新算法的攻击检测率高于 t 检验法，这是因为当参考簇选为弱攻击的簇时，参考簇均值与其余簇均值的差异之和较小。当 t 检验法的参考簇为受攻击簇时，$K=25$ 时，t 检验法的检测率与新算法相当；$K<25$ 时，t 检验法的性能好于新算法；$K>25$ 时，新算法的检测率高于 t 检验法。同时与二分比较法相比，无论 k 值多大，新算法的攻击检测率都较高。

4　结束语

该方法采用分簇结构，能获得较低能耗，且该方法计算复杂度低，攻击检测率较高。理论分析和仿真结果表明，新算法的攻击检测性能要优于现有的无线传感器网络攻击检测算法。

参考文献：

[1] Wagner D. Resilient aggregation in sensor networks[C]//In Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN). Washington DC, USA, 2004: 78-87.

[2] Buttyan L, Schaffer P, Vajda I. Resilient aggregation with attack detection in sensor Networks[A]. In Proceedings of the Fourth IEEE International Conference on Pervasive Computing and Communications[C]. Pisa, Italy, March 2006: 332-336.

[3] Luo Yongjian, Yang Xin, Zhang Xu. An effective resilient data aggregation algorithm in wireless sensor networks[A]. 2007 International Conference on Wireless Communication, Networking and Mobile Computing[C]. Shanghai, China, September, 2007: 2642-2646.

[4] Shu Qinren, Jong Sou Park. Density mining based resilient data aggregation for wireless sensor networks[C]. Fourth International Conference on Networked Computing and Advanced Information Management. 2008: 261-266.

[5] Luo Yongjian, Ding Xiaoyong, Wu Gang, et al. A novel attack detection algorithm based on t-Distribution in wireless sensor networks[A]. 2009 International Conference on Wireless Communications, Networking and Mobile Computing[C]. Beijing, China, 2009.

****

（上接第 17 页）

6　结束语

改性 B 炸药作为高膛压、高初速的大口径弹药的装药条件已经十分成熟，将极大提高我国大口径弹药的威力，同时也必将给我国的中大口径弹药带来一场新的变革，增强我军地面压制火炮在未来战场上的作战能力。

参考文献：

[1] 徐更光. 弹药高效毁伤关键技术集成与应用[J]. 含能材料, 2007, 26(增刊): 119-121.