第二届IEEE电力电子、智能控制和能源系统国际会议（ICPEICES-2018）

一种有效的加权信任方法

集群无线传感器网络中的恶意节点检测

|  |  |  |
| --- | --- | --- |
| 巴夫内什监狱  *电气工程系*  *德里理工大学*  印度德里  bhavneshmk@gmail.com  S、 印度河  *电子与通信工程系*  *德里理工大学*  印度德里  美国。indu@dce.ac.in | 维什瓦米特拉·辛格  *通信与电子工程系*  *德里理工大学*  印度德里  vishwamitra\_bt2k15@dtu.ac.in  尼塔·潘迪  *电子与通信工程系*  *德里理工大学*  印度德里neetapandey@dce.ac.in | 拉利特·库马尔·坦瓦尔  *电子与通信工程系*  *德里理工大学*  印度德里lalittanwar55@yahoo.com |

***摘要***

***关键词-w***

# 一、 简介

无线传感器网络（WSN）在应急响应系统、能源管理、医疗监控、后勤管理、库存管理和战场管理等领域有着广泛的应用[11]。无线传感器网络由一组称为传感器节点的小型设备组成。这些节点是配备传感器、处理单元、存储器单元、收发器和电源的便携式设备，如图1所示。传感器节点是特定应用的，用于监测特定参数，如温度、不同位置的污染物水平、化学品中的颗粒浓度、压力、声/光强度等。这些传感器随机部署在感兴趣的地理区域。传感器节点通过簇头节点和转发节点收集信息并发送到基站。传感器节点的电源有限，通常是一个电池，因此能力有限。假设转发节点具有高功率，它收集和处理来自下层传感器节点（SNs）和基站（BSs）的数据，这些节点充当无线传感器网络（WSN）和有线网络之间的媒介。集群是通过将作业区域平均划分为四个集群而形成的。每个簇头处理来自其下所有传感器点的数据，并将结果传递给转发节点。该方案基于

978-1-5386-6625-8/18/$31.00©2018 IEEE

假设转发节点和基站不是恶意的，因此总是可信的。

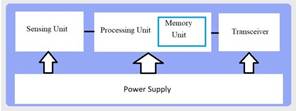


              图1。无线传感器网络传感器节点组件

由于传感器网络的无人值守特性，攻击者可以发起各种攻击并危害传感器节点。网络应该能够抵御这些攻击，如果攻击成功，其影响应该最小化。一个或几个传感器节点的损坏不应使整个网络崩溃。因此，必须对无线传感器网络的安全性和性能等关键问题进行研究。

在无线传感器网络中，针对恶意节点的检测，已有许多技术被提出。在无线传感器网络中，针对恶意节点的检测，已有许多技术被提出。由于电池寿命有限、内存空间有限和计算能力有限[1]、[2]、[3]，无线传感器网络可能会受到损害。为了防止恶意节点产生错误的结果，对其进行检测和隔离是非常必要的。没有明确结构的adhoc网络很难抵御任何类型的攻击，这可能导致节点容易受到攻击[4]。他们提出了一种方法，如果一个节点被它的邻居视为可信的，那么该节点将被声明为无故障的，并且不是恶意节点。然而，要使它工作，它必须有一个最小数量的节点附近，这是不能保证在传感器网络。

因此，杜、方、宁[6]提出了一种更好的方法，即让节点将周围其他节点的数据与节点自身生成的数据进行比较。如果数据之间的差异很小，那么节点就被认为是可信的。该方法对恶意节点的局部检测有较好的效果。

加权信任评估，主要用于检测恶意节点是相当可靠的。整个传感器节点被分配了一个频繁评估的权重或信任量。每次节点提供错误信息时，信任度都会降低。该方法将节点的信任度降低到一个固定的节点上。SNs将数据发送到转发节点。转发节点是高功率的，从SNs收集数据并进行处理并传输到基站。

该方案基于一个关键假设，即转发节点和基站都不会出现故障，因为一旦进入故障转发节点，它就可以在网络中发动攻击[9][10][7]。[15] 在MATLAB环境下进行了广泛的加权信任评估仿真，重点是响应时间和检测率[13][14]。针对WSN中的安全问题，描述了各种攻击[17]描述了网络中的各种分簇算法，这些分簇算法描述了一种高效的传感器节点定位和提高可靠性的方法。

本文研究了利用加权信任评估方法检测恶意传感器节点所需的传播时间。我们比较了传统的加权信任评估方案[5]（一个由传感器节点、转发节点和基站组成的三层分层网络）和一个提出的基于簇的加权信任评估（混合拓扑感知节点、簇头、转发节点和基站）所用的时间。

论文的其余部分安排如下。第二节介绍了无线传感器网络的安全性及相关工作。第三节介绍了全文所使用的网络模型和体系结构。第四节提出了基于聚类的加权信任评估方案。仿真结果见第五节。本文的结论在第六节。

# 二。无线传感器网络的安全性

无线传感器网络的安全性至关重要，设计无线传感器网络时面临的挑战如下：

**恶劣环境**：传感器节点面临极其恶劣的环境条件，当传感器节点暴露在开阔区域时，很容易受到破坏或被攻击者捕获。攻击者可以捕获传感器节点并访问数据或通过它们传输假数据。

**无人值守操作**：传感器节点部署在敌对区域，使其暴露在物理回火和攻击之下。

**有限的资源**传感器节点的安全性需要能量、内存和存储容量等资源，因为数据是不断被监视和/或记录的。传感器资源的短缺给资源密集型安全机制带来了挑战。这些资源在一个小的传感器节点中非常有限。

**无线通信的可靠性**在无线传感器网络中，由于信道错误，传感器数据可能会失真，从而导致冲突，在高繁忙节点上，传感器数据也可能失真，从而容易发起拒绝服务（DoS）攻击。由于单个节点的拥塞更大，过载导致传感器网络的延迟增加，从而导致同步错误和系统延迟，包括传感器节点。攻击者可以通过恶意节点在传感器网络中发起攻击。这些攻击大致分为被动攻击和主动攻击。被动攻击比较容易分析，也很难被发现。在被动攻击中，攻击者不修改或交换信息，这种类型的攻击基本上是为了寻找一些机密信息的知识[12]。

在主动攻击中，攻击者试图更改传感器节点传输的数据，或通过插入流量来使传感器过载，从而启动拒绝服务攻击。

# 三、 网络模型与体系结构

网络模型基本上有两个组成部分，即WSN组件和WSN网络拓扑。部件说明如下：

## A、 无线传感器网络的组成

大气污染环境监测无线传感器网络由分布在现场的传感器点或传感器节点组成。这些传感器节点由检测和监测环境中污染物浓度的传感器组成。这些传感器节点通过无线链路连接到簇头，簇头处理来自每个单独节点的收集的读数，并将这些数据转发给转发节点，该转发节点再次处理来自各个簇头的收集的读数并将其传播到图2所示的基站。

## B、 网络拓扑

在无线传感器网络中，我们提出了一种基于星型、网状和环形拓扑的混合网络拓扑结构。这三种拓扑结构用于增加系统的多功能性，同时考虑到以下可用资源[16]：

•一组感测节点连接到一个中心节点，即集群头，该节点具有其他能力，如从其他簇头进行连接和数据交换，这包括星形拓扑，因此产生一组簇。星型拓扑与其他拓扑相比具有优势，包括其可扩展性和功耗降低。

•簇头作为网状物连接在一起，以提供可靠的通信，簇头有额外的资源，便于使用此类拓扑。所有簇头直接连接到转发节点，转发节点充当从无线到有线网络（即到外部世界）的路径。图2描述了使用混合网络拓扑的WSN的总体架构。

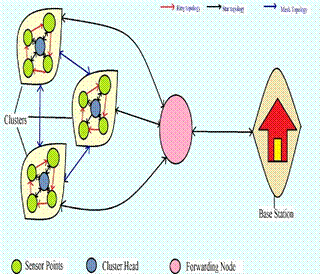


              图2。系统架构

## C、 误差检测与减重公式

在检测恶意节点时，利用传感器节点的信任值来反映其在决策过程中的跟踪记录。每个簇头维护其关联传感器节点的信任值。信任值（𝑉𝑤）在范围（0,1）内，并为每个传感器节点初始化为1。权重代表传感器节点的可靠性，权重越高的节点越可信。更新信任值对于保持传感器读数的保真度非常重要。为了确定无误节点，加权阈值应大于最小阈值。

𝑉𝑡ℎ𝑤

𝑀 − | 𝐷|

𝑉𝑤 =

𝑀

式中，𝑉𝑡ℎ为最小阈值权重，𝑉𝑤为加权阈值。M是传感器在某一点的平均值或平均值。（M是用户定义的值）。D是与M的偏差。D取决于传感器输入值，可计算为（𝑀−𝐼）。其中I是来自传感器的输入值。

例如，在热带雨林中，温度在21到30度之间变化，那么平均值（M）为25.5度。如果某个特定的传感器检测到当时的温度，则检测值为I。让检测值为34度。现在计算出的阈值是

34 |𝑉𝑤=



因此，𝑉𝑤计算为0.67。假设最小阈值设为0.7，则方程式𝑉𝑡ℎ𝑤不满意。因此，对应的传感器节点是错误节点。

**重量修正**

如果发现传感器节点错误，则根据以下公式减少权重。

𝑊′ = 𝑊 + 𝐹 × 𝑊

式中，𝑊′是修改后的权重，W是当前权重，F是权重惩罚因子。

四、 基于聚类的加权信任评估

其目标是提出一个增强的加权信任评估方案的原型，用于检测恶意传感器节点和簇头。该方案需要满足的性能要求是响应时间短、检测率高、误报率低。响应时间是指该方案正确检测到恶意节点所需的平均周期数，检测率是指该方案正确检测到的恶意节点占WSN中存在的恶意传感器节点总数的比率。现场随机部署多个传感器节点n，其中一个子集被选为转发节点，其余节点则成为普通传感器节点（SN）。传感器节点将自己组织起来，形成一个集群的操作网络。

# 五、 模拟结果

在集群节点中安装了基于WTE的检测算法，对所有成员传感器节点进行监控。

                        表1.模拟参数

|  |  |
| --- | --- |
| 最小阈值权重 | 0.7 |
| 集群数量 | 4 |
| 样品重复次数 | 5 |
| 网络字段维度 | 100×100 |
| 现场传感器节点 | 100 |
| 权重惩罚因子 | 20% |
| 部署时的恶意节点 | 20% |

虽然现场参数是用户输入，但是在[100x100]的区域内随机部署了由上百个传感器节点组成的异构网络，仿真结果如图4所示

将传感器分组在簇中，并对其进行加权信任评估算法。如图5所示，恶意节点显示在各自的集群中。此方法执行了5次，传播时间在图6中进行了比较。结果表明，随着样本数的增加，传播时间随聚类次数的增加而减小，而在无聚类的情况下，传播时间增加。

## 图3。加权信任评估算法

虽然现场参数是用户输入，但是在[100x100]的区域内随机部署了由上百个传感器节点组成的异构网络，仿真结果如图4所示

将传感器分组在簇中，并对其进行加权信任评估算法。如图5所示，恶意节点显示在各自的集群中。此方法执行了5次，传播时间在图6中进行了比较。结果表明，随着样本数的增加，传播时间随聚类次数的增加而减小，而在无聚类的情况下，传播时间增加。

**检出率：**

检测比率（DR）是检测到的恶意节点数与网络中恶意节点总数之间的比率（在部署时设置）。在一次模拟运行中，恶意节点的百分比设置为20%（m=0.2）。这意味着：

恶意节点=20/100\*n

其中n=部署的传感器节点数，即=100。

恶意节点=20

还有一组恶意节点是集群头

恶意簇头=m\*（p\*n）

=20/100\*（4/100\*100）=0.8=1

其中p=网络中簇头的百分比=4/100。

表二。参数与节点

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 完全恶意的  节点  （在  部署） | 20 | 40 | 60 | 80 |
| 检测  恶意的  节点  （模拟） | 18 | 33 | 38 | 29 |
| 检出率（DR） | 0.9 | 0.83 | 0.63 | 0.36 |

恶意普通传感器节点=m\*（n-（p\*n））

=20/100\*（100–（4/100\*100））=19.2=19

在19个被设置为恶意的节点中，检测到的恶意普通传感器节点数为17个，而所有的恶意簇头都是通过该方法检测到的。

检测率=正确检测到的恶意节点数/网络中恶意节点总数。

DR=（17+1）/20=0.90

在图7中，我们绘制了恶意节点数与检测率的关系图。观察到恶意节点的检出率随检测率的增加而降低。

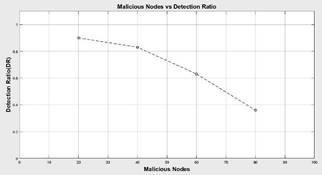


                           图7。恶意节点与检测率

# 六、 结论

仿真结果表明，第二种情况下（单独考虑单个集群而不是同时考虑整个区域）的传播时间要小得多（少了近11倍），当考虑部署时有20个恶意节点时，检测到90%的恶意节点。如果簇的数目增加，那么检测率就会增加。

文中给出了仿真结果，结果表明，该算法可以灵活地应用于在簇头下工作的传感器节点数目，从而在可观的检测率和较短的传播时间下获得了较好的可扩展性。

## 参考文献

[1] E.Ayday、F.Delgosha和F.Fekri，“使用网络编码的无线传感器网络的位置感知安全服务”，Infocom，2007年5月。

[2] S.Zhu、S.Setia和S.Jajodia，“LEAP：大规模分布式传感器网络的有效安全机制”，CCS&apos;032003年10月。

[3] C.Karlof、N.Sastry和D.Wagner，“TinySec：无线传感器网络的链路层安全架构”，ACM Sensys，2004年11月。

[4] 罗海云，郭杰军，陆松武，张丽霞，“自保护无线自组网”，2002年，意大利。

[5] 胡红兵，陈宇，辜伟新，苏周，“基于加权信任评估的无线传感器网络恶意节点检测”，SpringSem，第836-8432008页。

[6] 杜文华，方立群，宁平，“无线传感器网路之定位异常侦测”，第十九届国际并行与分布式处理研讨会（IPDPS&apos;05），2005年4月3日至8日，美国科罗拉多州丹佛市。

[7] I.M.Atakli，H.Hu，Y.Chen，W.S.Ku和Z.Su，无线传感器网络中的恶意节点检测，系统安全模拟研讨会（SSSS&apos;08），加拿大渥太华，第838页，2008年。

[8] 赵S，K.Tepe，I.Seskar和D.Raychaudhuri，自组织分层自组织无线网络路由协议，IEEE Sarnoff研讨会论文集，新泽西州特伦顿，2013年3月。

[9] K.Sumathi和D.M.Venkatesan，一项关于检测无线传感器网络中受损节点的调查，（IJCST）国际计算机科学与信息技术杂志，第5卷，第7720-7722页，2014年。H.Hu，Y.Chen，W.-S.Ku，Z.Su和C.-H.J.Chen，无线传感器网络中基于加权信任评估的恶意节点检测，《国际信息与计算机安全》，第3卷，第2期，第148页，2009年。

[10] R.Sharma和N.Tripathi，《无线传感器网络综合评论》，《东方计算机科学与技术杂志》，第8卷，第1期，第59-64页，2015年4月。

[11] D.G.Padmavathi和M.D.Shanmugapriya，无线传感器网络中的攻击、安全机制和挑战调查，国际计算机科学与信息安全杂志，2009年第4卷。

[12] Rajkumar，Vani B.A.，G.Rajaraman，Dr.H.G.Chandrakanth，“无线传感器网络中的安全攻击及其对策”，国际工程研究与应用杂志，第4卷，第10期（第1部分），第04-15页，2014年10月。

[13] Mohamed Lamine Messai“无线传感器网络攻击分类”国际电信和

申请书14阿尔及利亚A.MIRA Bejaia大学，2014年4月23日至24日。

[14] Koriata P.Tuyaa和W.Okelo-Odongo，“用于检测无线传感器网络中恶意节点的增强加权信任方案”，《国际计算机应用杂志》（09758777），第155卷第4期，2016年12月。

[15] T.Sathyamoorthi，D.Vijayachakaravarthy，R.Divya And M.Nandhini，一种简单有效的无线传感器网络恶意节点发现方案，国际工程技术研究杂志，第03卷，第02期，2014年。

[16] 刘晓明、史俊杰，“无线传感器网络中的分簇路由算法：综述”，《互联网与信息系统KSII汇刊》，第6卷，第7期，2012年：第1735-1755页。