文章编号:1671-4598(2014)08-2673-04　　中图分类号:TP393　　文献标识码:A

# 无线传感器网络 AMRSSI 加密调制定位算法研究

王　伟，王召巴
（中北大学 信息与通信工程学院，太原　030051）

**摘要**：RSSI 定位技术在无线传感器网络实际应用中，由于环境的开放性，信号很容易受到敌方的攻击，从而使系统的定位产生错误；通过对 RSSI 测距定位模型进行分析，提出了基于 RSSI 新的加密调制定位算法 AMRSSI，该定位算法计算简单、保密性强、受外界干扰小；仿真实验表明该算法较普通的基于 RSSI 的测距方法定位精度上有了明显的改进，适合在通信开销小、硬件要求低的传感器网络节点上应用。

**关键词**：无线传感器网络；RSSI；调制；加密；抗攻击

# Research of RSSI－AM Encryption Modulation Localization Algorithm in Wireless Sensor Networks

Wang Wei, Wang Zhaoba
(School of Information and Communication Engineering, North University of China, Taiyuan　030051, China)

**Abstract**: In practical application of wireless sensor networks, because of open environment, signal is easy to be attacked and traditional RSSI location technology produces errors. By analyzing the location modal of RSSI, this paper proposes a new encryption modulation algorithm: RSSI－AM, which is unlike most approaches. The location algorithm has the following advantages: simple calculation, strong security, powerful anti－interference ability and no hardware expansion required. Besides, the simulation experiment shows the location precision of ranging method based on RSSI－AM has obvious improvement compared with traditional algorithm. It can be used in the environment of wireless sensor network nodes with low cost and performance of hardware.

**Keywords**: wireless sensor networks; RSSI; modulation; encryption; anti－attack

## 0　引言

无线传感器网络是由大量具有数据采集、数据处理和无线通信能力的传感器节点构成的无线自组织网络，其目的是协作地感知、采集和处理网络覆盖的区域内感知对象的信息，并传送给主控端，从而进行系统决策和控制。

在无线传感器网络中，传感器节点的位置信息整个网络中信息获取和信息处理的重点。目前已经有很多系统和算法致力于研究 WSN 的定位技术，但是由于无线传感网络的很多应用是处在开放性的环境中，所以定位系统非常容易受到外部的信号干扰，甚至是外部攻击。为了能够提供一个安全有效的网络，就需要针对无线传感器网络的定位算法进行一个安全防护，目前也有很多研究者提出了相关的一些算法，提出的各种安全定位算法针对性比较强，都是侧重于某个特定的攻击，如果攻击类型发生变化，则其防护性能将会失效。而且目前的大部分算法主要研究的是防范恶意攻击技术，而在实际应用环境中有许多不可避免的其它信号干扰，也是必须要考虑防范的因素[1-3]。

**收稿日期**:2014-05-07；　**修回日期**:2014-06-16。
**基金项目**:山西省青年科技研究基金(2013021015－2)。
**作者简介**:王伟(1978-)，男，博士，讲师，硕导，主要从事无线传感器网络、传感器检测、信息与信号处理方向的研究。
王召巴(1967-)，男，博士，教授，院长，博导，主要从事传感器检测技术、信息与信号处理方向的研究。

## 1　无线传感器网络定位技术

无线传感网络中的定位是指在网络中一个节点如何获取自身的地理位置信息。目前大多数的无线传感网络都采用了分布式定位技术，它的基本原理就是：在网络中包含少量的信标节点（beacon node）也称之为锚节点，这些节点通过自身携带的 GPS（global position system）定位组件来获得自身的位置信息，然后发送位置参照信息，并且建立坐标系，在网络中的其它未知节点首先测量或者估算自身与信标节点的位置关系，包括距离、角度和区域包含关系，然后利用这些关系和特定的算法计算出未知节点的位置。常用的计算位置的算法有三边测量、三角测量和极大似然估计等。

根据定位发现机制，可以把 WSN 的定位方法分成两种：距离相关和距离无关。距离相关的算法通过测量节点间点到点的距离或者角度信息，然后通过数学方法进行节点位置计算，目前常用到的有基于到达时间的算法（TOA）、基于到达时间差的算法（TDOA）、基于到达角度的算法（AOA）及基于接受信号强度指示算法（RSSI）等。距离无关的算法不需要距离和角度信息，而是通过网络连通性等信息实现节点定位，目前常用到的算法有质心算法、凸规划、DV－HOP 及 APIT 等。上述这些算法都是在理想环境下进行定位，并没有考虑外界因素对系统的定位影响[4-6]。

## 2　RSSI 算法分析

RSSI 是在已知发射功率的情况下，通过接收节点测量接收功率，利用接受节点接收功率的损耗来计算传播损耗，最后

把传播损耗用理论或者经验上的信号传播模型转化为距离。

首先从数学上了解一下 RSSI 的测距基本原理。传感器节点的无线信号的发射功率与其接收功率之间的数学关系可以用公式（1）表示，公式中无线信号的接收功率用 $P_R$ 表示，无线信号的发射功率用 $P_T$ 表示，收发单元之间距离用 $r$ 表示，传播因子用 $n$ 表示，无线信号传播环境对传播因子数值大小有着很大的影响。

信号传输理论模型常采用无线电传播损耗模型来进行分析，信号的经验模型是建立各个点上的位置与信号强度的数据库进行匹配。一般选择自由空间传播损耗模型和对数常态分布模型来进行计算。自由空间传播损耗模型如下：

$$PL(d_0) = 32.44 + 10n\lg d_0 + 10n\lg f \tag{1}$$

其中：$PL(d_0)$ 为无线传输距离 $d_0$ 路径损耗，$n$ 为路径损耗因子，$f$ 为信号频率。

对数常态分布模型如下：

$$PL(d) = PL(d_0) + 10n\lg(d/d_0) + \xi \tag{2}$$

其中：$PL(d)$ 为传输距离为 $d$ 的路径损耗，$PL(d_0)$ 为传输距离 $d_0$ =1 m 时的路径损耗，$n$ 为信号的衰减系数，一般取值在 2～5 之间，$\xi$ 是均值为 0 的高斯随机分布函数[7-11]。

位置节点接收参考节点的信号强度为：

$$RSSI = P_s + P_a - PL(d) \tag{3}$$

其中：$RSSI$ 为接收到的功率，$Ps$ 为节点发射功率，$Pa$ 为天线增益，$PL(d)$ 为路径损耗。

把式（1）、（2）带入到式（3）中，得到：

$$RSSI = P_s + P_a - [32.44 + 10n\lg d_0 + 10n\lg f + 10n\lg(d/d_0) + \xi] = P_s + P_a - 32.44 - \xi - 10n(\lg d + \lg f) \tag{4}$$

设参数 $M = P_s + P_a - 32.44 - \xi$，则式（4）为：

$$RSSI = M - 10n\lg df \tag{5}$$

在无线传感器网络中，由于 $RSSI$ 信号是在空间中传播，其不仅具有一个传播衰减的特征，而且有可能会受到空间中其他信号的干扰。更严重的情况是如果有恶意入侵存在，正常的 $RSSI$ 信号会受到故意的干扰，导致节点接收到 $RSSI$ 信号与实际不符，从而使节点定位出现偏差。针对这样的实际问题提出一种解决方法，可以通过改进算法提高系统的抗干扰和抵御恶意攻击的能力。

首先在无线传感器网络布置过程当中，通过对节点接收到的多个 $RSSI$ 进行求差，如下计算：

$$RSSI_1 - RSSI_2 = (M_1 - 10n\lg d_1 f_1) - (M_2 - 10n\lg d_2 f_2) = M_1 - M_2 + 10n\lg \frac{d_2 f_2}{d_1 f_1} \tag{6}$$

当无线传感器网络中的节点的发射频率、发射功率、天线增益及路径损耗增益相同的时候得到：

$$RSSI_1 - RSSI_2 = 10n\lg \frac{d_2}{d_1} \tag{7}$$

同理，可以得到其它相关两个节点之间的 $RSSI$ 差值的关系，通过相关节点 $RSSI$ 的差值来进行信号位置信息的传输。

## 3　数据加密 AMRSSI 算法研究

基带调制信号与载波进行调制得到已调波或称为已调信号。已调信号通过信道传送到接收端，在接收端经解调后恢复成原始基带信号。解调是调制的反变换，是从已调波中提取调制信号的过程。调制解调信号通信系统，不仅优化了接收和发射机的硬件要求，而且在传输过程中减小了干扰和攻击损害。在无线传感器网络中用节点接收到的 $RSSI$ 差值信号进行调制，从而提高系统的信息传输的抗干扰和攻击的能力，利用式（7）进行调幅，如下：

设载波信号为：

$$y = A\cos\omega t \tag{8}$$

其中：$A$ 为信号的幅度，$w$ 为信号的角频率。

用 RSSI 的差值对载波进行幅度调制，可以实现较远距离的传输，而且载波的频率可变，从而在开放环境中不容易受到恶意攻击，其调制结果为：

$$y = 10An\lg \frac{d_n}{d_1}\cos\omega t \tag{9}$$

其中：$n$ 为无线传感器网络中对应的节点编号。在式（9）中 $\frac{d_n}{d_1}$ 为离散值，在实际应用中，系统采用一个定时器，使信号在一个载波周期内保持一个幅值不变。

由 $RSSI$ 的基本理论可知，至少需要 3 个已知位置信息的锚节点来定位未知节点的位置，但是如果一个锚节点遭到了破坏，那么将无法获得未知节点的位置信息，可以通过增加整个无线传感器网络系统内的锚节点与未知节点的关系，也就是增加未知节点定位的依赖条件，从而提高网络对于攻击的抵御能力。根据参考文献［7－11］，系统在 10 个锚节点定位的情况下就可以达到较高的定位效果，如图 1 所示，可以通过 10 个锚节点与位置节点的关系来进行定位。利用 Matlab 建立了一个在 50 m×50 m×50 m 的范围内统一的仿真环境，锚节点分布在这个范围内，根据 10 组 $RSSI$ 的差值，1.5，1.7，1.9，2.3，2.5，2.9，3.3，3.7，3.8，3.9，$f$=250 Hz，$A$=1 m 对式（9）进行 Matlab 仿真，对差值进行一定规律的分布，其规律也就是加密的方法，然后进行调幅。把定位信息转化为密文，形成加密秘钥，在接收端通过解密密钥进行识别。目前的加密算法主要采用对称密钥算法或者非对称密钥算法，这两种算法的计算复杂程度比较高，安全性比较好，但是由于无线传感器网络中传感设备可以利用的资源有限，所以采用一种代换算法进行加密。

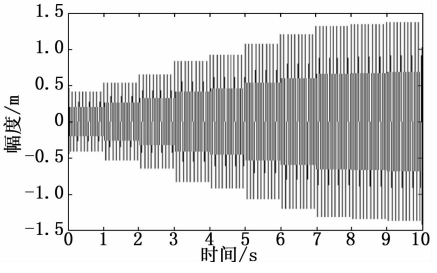


图 1　10 组 $RSSI$ 差值调制

将数据按照正常顺序进行排列，使之与 3，4，5，6，7，8，9，0，1，2（此时密钥为 3）分别对应，对上文的 10 个 $RSSI$ 差值信号进行代换加密：

明文：1.5，1.7，1.9，2.3，2.5，2.9，3.3，3.7，3.8，3.9

一次密文：3.7，3.9，3.1，4.5，4.7，4.1，5.5，5.9，5.0，5.1

然后将一次密文与 5，6，7，8，9，0，1，2，3，4（此时密钥为 5）对应相加，得到二次密文：

二次密文：8.7，9.9，10.1，12.5，13.7，4.1，6.5，7.9，8.0，9.1

然后根据 5－3＝2（此时 2 为密钥），将二次密文中 2 的整数倍的数据，也就是第 2，4，6，8，10 位的数据进行移位，得到了三次密文：

三次密文：8.7，9.1，10.1，9.9，13.7，12.5，6.5，4.1，8.0，7.9

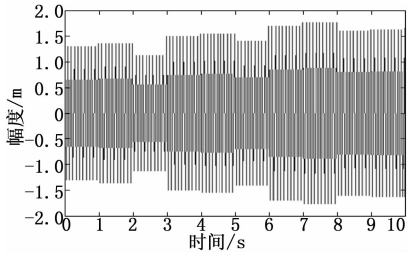


图 2　一次加密

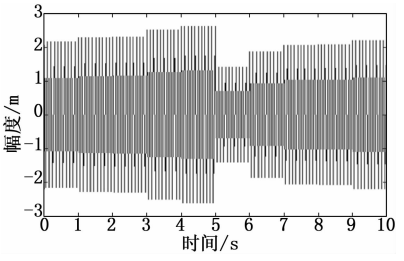


图 3　二次加密

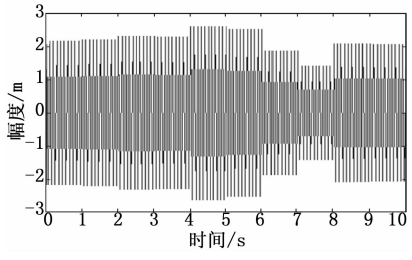


图 4　三次加密

原始数据经过 3 次加密其幅度和位置顺序都发生了变化，攻击者的解密难度比较大，而且算法本身的计算复杂程度并不高，满足了无线传感器网络硬件限制要求，不会占用太大的计算资源，能耗较小，具有较好的保密性。

接收端的接收机对其进行解调，对收到的已调制信号进行包络检波，得到结果如图 5 所示。

然后对解调信号进行解密，其过程就是加密的逆过程，根据密钥 3 和 5 对密文进行 3 次逆变换就可以得到发射端的 $RSSI$ 差值信息，也就是明文：1.5，1.7，1.9，2.3，2.5，2.9，3.3，3.7，3.8，3.9。

根据接收端的同步时钟对接收到的 $RSSI$ 差值信号进行处理：

$$E = RSSI_1 - RSSI_2 = 10An\lg\frac{d_2}{d_1} \tag{10}$$

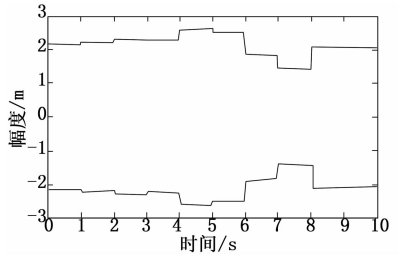


图 5　包络检波解调信号

$$d = \frac{d_n}{10^E} \tag{11}$$

其中：$E$ 为节点接收到的 $RSSI$ 差值，$d_n$ 为已知的其它节点到目标节点之间的距离，通过上式可以得到对应的距离 $d$ 。

## 4　参数性能比较

为了比较 RSSI－AM 定位节点算法和传统的 RSSI 定位算法的性能，利用 Matlab 建立了一个在 50 m×50 m×50 m 的范围内统一的仿真环境，锚节点均匀地分布在这个范围内，每一个未知节点都可以接收到全部锚节点的信息。锚节点周期发送自身信息。仿真采取对 100 个在测试范围内平均分布的未知节点结果取算术平均作为最后的结果，仿真结果如图 6 所示。

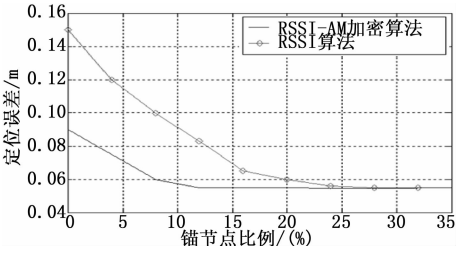


图 6　算法定位精度比较

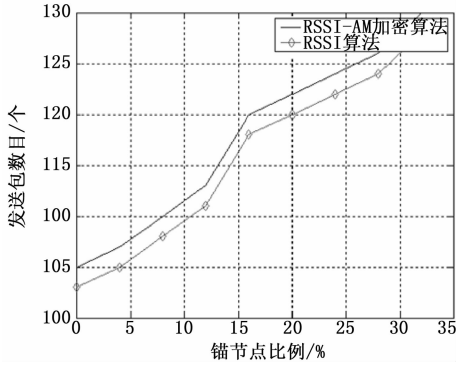


图 7　算法通信量比较

如图 6 显示，在锚节点比例小于 16%时，AMRSSI 算法定位精度明显高于 RSSI 算法，随着锚节点的增加，两种算法的定位精度都不断得到提高。当锚节点比例趋近 30%，定位精度趋近恒定值。

图 7 是 ERSS 测距算法和 RSSI 测距算法通信量比较，图中显示 RSSI－AM 算法相对于 RSSI 增加了一定的通信开销，但是增加量并不大，不会对通信产生太大的负担。

## 5 结束语

本文提出了一种基于 RSSI 的传感器网络定位加密调制算法 AMRSSI，该算法首先通过 RSSI 基本测距原理以及空间传播损耗模型和对数常态分布模型，推导出未知节点和锚节点的关系，为了适应无线传感器网络生存的复杂环境和敌对攻击，算法对数据进行加密，然后利用 RSSI 的差值对载波幅度进行调制，在接收端通过包络检波和解密得到 RSSI，再通过极大似然估计法得到节点的位置信息。该算法对硬件的要求不高，适用于大多数无线传感器网络定位的测距要求。

**参考文献：**


[1] Chan H，Perrig A. Security and Privacy in Sensor Networks [J]. IEEE Computer，2003，36 (10)：103－105.

[2] Capkun S，Cagalj M，Srivastava M. Secure localization with hidden and mobile base stations [A]. Proc. of the 25th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM' 06) [C]. Barcelona，Spain，2006：23－29.

[3] Anjum F，Pandey S，Agrawal P. Secure localization in SN using transmission range variation [A]. Proc. of the 2nd IEEE Intenational Conference on Mobile Ad－hoc and Sensor System (MASS' 05) [C]. Washington DC，2005.

[4] Lazos L，Poovendran R. SeRLoc：Secure range－independent localization for wireless sensor networks [A]. Proc. of the 2004 ACM Worksho Pon Wireless Security (WISE' 04) [C]. Brisbane，Australia，2004：21－30.

[5] Lazos L，Poovendran R，Capkun S. ROPE：Robust position estimation in wireless sensor networks [A]. Proc. of the International Symposium on Information Processing in Sensor Networks (IPSN' 05) [C]. Los Angeles，CA，2005：324－331.

[6] Lazos L，Poovendran R. HiRLoc：High－resolution robust localization for wireless sensor networks [J]. IEEE Journal on Select－ed Areas in Communications，2006，24 (2)：233－246.

[7] Ekici E，Vural S，McNair J，et al. Secure probabilistic location verification in randomly deployed wireless sensor networks [J]. Ad Hoc Networks，2007.

[8] Du W L，Fang L，Ning P. LAD：Localization anomaly detection for wireless sensor networks [J]. Journal of Parallel andDistributed Computing，2006，66 (7)：874－886.

[9] Liu D G，Ning P，Du W L. Detecting malicious beacon nodes for se－cure location discovery in wireless sensor networks [A]. Proc. of the 25th International Conference on Distributed Computing System (ICDCS' 05) [C]. Columbus，Ohio，2005：609－691.

[10] Li Z，Trappe W，Zhang Y，et al. Robust statistical methods fosecuring wireless localization in sensor networks [A]. Proc. othe International Symposium on Information Processing in Sensor Networks (IPSN' 05) [C]. Washington，2005：91－98.

[11] Liu D G，Ning P，Du W L. Attack－resistant location estimation in sensor networks [A]. Proc. of the International Conference on Information Processing in Sensor Networks (IPSN' 05) [C]. Lo Angeles，CA，2005：99－106.


(上接第 2672 页)

CHDFS 系统中，在图片数量相同的情况下，Namenode 内存中元数据个数得到有效控制，Datanode 中数据块空间得到了有效利用。

从对比结果看，基于 Cache 的海量图片存储优化方案 CHDFS 确实达到了预期的目的。

## 4 结语

HDFS 是针对大文件存储而设计的分布式文件系统，用它来存储海量的图片时，会造成严重的性能瓶颈，浪费大量的存储空间。本文针对此问题，提出了基于 Cache 的海量图片存储优化方案。该方案改变了 HDFS 原来的 Namenode 和 Datanode 两层设计模式，在 HDFS 中引入 Cachenode，提出了现在的 CacheNode、Namenode 与 Datanode 3 层设计模式。该设计方案集成了 Cache、预读、图片合并等有效机制，共同用来提高海量图片在 HDFS 中的读写性能，弥补了 HDFS 存储海量图片时的缺陷。由于 Cache、预读以及图片合并等操作对用户都是透明的，所以，该方案并没有增加用户使用 HDFS 的复杂性。实验表明，本方案用于海量图片的存储是切实可行的。下一步工作就是通过数据挖掘，使得图片合并的算法更加高效合理，提高 Cache 命中率，使得存储效率的提高更加显著。

**参考文献：**


[1] 蔡睿诚. 基于 HDFS 的小文件处理与相关 MapReduce 计算模型性能的优化与改进 [D]. 吉林：吉林大学，2012：

[2] 王玲惠，李小勇，张轶彬. 海量小文件存储文件系统研究综述 [J]. Computer Applications and Software，2012，29 (8)：106－109.

[3] 马 灿，孟 丹. 曙光星云分布式文件系统：海量小文件存取 [J]. Journal of Chinese Computer Systems，2012，33 (7)：1481－1488.

[4] Zhang Y，Liu D. Improving the efficiency of storing for small files in hdfs [A]. 2012 International Conference on Computer Science and Service System，CSSS 2012 [C]. 2012：2239－2242.

[5] Linux 公社：MapReduce 及 Hadoop 国内外研究概况 [EB/OL]. http：//www. linuxidc. com/ Linux /2012 － 03/56687. htm，2013－05－13：

[6] chinaz：Facebook 大数据：每天处理逾 25 亿条内容和 500TB 数据 [ EB/OL ]. http：//www. chinaz. com/news/2012/0823/270885. shtml，2013－04－12：

[7] Apache：The Apache Software Foundation. HDFS Architecture [EB/OL]. http：//hadoop. apache. org/docs/current/hadoop－project－dist/hadoop－hdfs/HdfsDesign. html，2013－04－12：

[8] Zhou L，Fang Z Y，Xiang L Y，et al. Performance optimization of processing small files based on HDFS [J]. International Review on Computers and Software，2012，7 (6)：3386－3391.

[9] Dong B，Zheng Q H，Tian F，et al. An optimized approach for storing and accessing small files on cloud storage [J]. Journal of Network and Computer Applications，2012，35 (6)：1847－1862.