基于 RSSI 的传感器网络节点安全定位机制

叶阿勇，许力，林晖

（福建师范大学 密码技术与网络安全重点实验室，福建 福州 350007）

摘 要：针对 RSSI 测距存在的脆弱性问题，提出了一种基于完整性编码和不间断占用信道的安全 RSSI 测距协议，该协议不仅可以抵抗伪造插入、重放/虫洞等常规攻击，而且可以防止信标信号被恶意干扰而削弱，即可抵抗虚增测距的外部攻击。在此基础上，设计了一种基于 RSSI 的传感器网络节点安全定位机制，该机制采用可校验的多边测量法来过滤虚减测距的外部攻击，实现安全定位，并对测距协议和定位机制的安全性进行了理论分析。

关键词：无线传感器网络；节点定位；安全定位

中图分类号：TP393.4 **文献标识码**：B **文章编号**：1000-436X(2012)07-0135-08

Secure RSSI-based node positioning mechanism for wireless sensor networks

YE A-yong, XU Li, LIN Hui

(Key Lab. of the Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China)

Abstract: For securing the RSSI-based ranging, a new protocol was proposed firstly, which achieved robustness by applying integrity coding and occupation of communication channel. The theoretical analysis showed the proposal was resilient to most conventional attacks including signal forgery and replay, also it can prevent adversary from attenuating the ranging signal, which reducing the measured distance. Furthermore, a new secure node positioning scheme for sensor networks was proposed by applying the proposed protocol above, in which, the distance enlargement attacks were further filtered out by verifiable multilateration. The detailed analysis was also given to shown it's robustness under external attacks.

Key words: wireless sensor networks; node positioning; secure positioning

1 引言

节点的安全定位是传感器网络可靠运行和收集可信数据的重要前提。近年来，研究者提出了许多节点安全定位机制和算法，如基于 VM 的安全定位[1]、SeRLoc[2]、SLA[3]、基于隐蔽基站的安全定位[4]、基于顽健计算的安全定位算法[5,6]等。然而现有的安全定位机制所依赖的前提条件和假设是传感器网络难以满足的。例如，VM 算法采用的距离界限协议需要验证者具有纳秒级的时间测量能力和被验证者具有纳秒级的实时处理能力，SeRLoc 要求每个信标节点都配置精确的定向天线，而基于顽健计算的定位机制往往要求节点运行复杂的启发式搜索算法。由于受成本和功耗等因素的限制，典型传感器节点的计算能力和硬件配置都十分有限，其内置时钟都只能达到微秒级测量精度。例如，智能尘埃[7]配置为：8bit 4MHz 的 CPU，512byte 的 RAM，512byte 的 EEPROM，10kbit/s 的通信速率，

收稿日期：2011-08-22；**修回日期**：2011-11-08

基金项目：国家自然科学基金资助项目（61072080）；福建省自然科学基金资助项目（2009J01274, 2010J05128, 2011J01339）

Foundation Items: The National Natural Science Foundation of China(61072080); The Natural Science Foundation of Fujiar Province (2009J01274, 2010J05128, 2011J01339)

4kbyte 的代码空间。由此可见，现有的安全定位机制并不能适应低功耗、低成本的传感器网络应用。

文献[8]提出了一种完整性编码机制（I-Codes, integrity codes）用于保护在不安全信道中传递消息的完整性。I-Codes 是在曼彻斯特编码的基础上，采用基于随机信号的调制技术来传输消息。受曼彻斯特编码的约束，任何篡改攻击至少要将报文中的一位“1”改为“0”才能避免消息编码违例，但由于随机信号难于被湮灭，攻击者无法擦除信道中基于随机信号输出的码字“1”，因此，I-Codes 在不依赖密码技术的情况下可保护消息的完整性。Rasmussen 等人在 SecNav 系统中最先将 I-Codes 应用于无线安全定位与时间同步[9]，SecNav 利用 I-Codes 的安全特性来防范伪造插入、重发攻击和虫洞攻击。但 SecNav 是基于 TOA 测距技术，要求节点具备纳秒级的时间测量精度和多通道并行通信能力，因此也不适用于资源严格受限的传感器网络。

本文中，首先基于 I-Codes 和信道不间断占用策略设计了一种具有安全下界的 RSSI 测距协议。在此基础上，采用可校验的多边测量法和信道复用技术，设计一种安全的节点定位算法（SeRLA, secure RSSI-based localization algorithm）。

2 预备工作

本节定义了 SeRLA 所适用的系统模型和相关假设，并分析了 RSSI 测距的安全性和可能受到的攻击方式。

2.1 系统模型与相关假设

本文旨在为无线传感器网络提供安全的节点定位解决方案，因此分析问题主要侧重于如何提高定位的安全性。以下假设适用于本文方案：1）传感器网络由大量传感器节点、若干个信标节点以及一个汇聚节点组成，并且每个节点均有唯一的标识符 ID；2）网络的部署区域为一个平面，因为平面中，信标节点的信号覆盖范围可近视为一个圆，且每个传感器节点只需接收到 3 个不同的信标即可定位；3）网络采用随机方式部署传感器节点，并可按一定策略精确部署信标节点，信标节点可借助 GPS、手工预设或有线网络实现自身的定位和时间同步（纳秒级）；4）每个传感器节点与 Sink 节点共享一个预设密钥，用于相互间的保密通信。

2.2 RSSI 测距的安全分析

RSSI(received signal strength indication)是一种常见的低成本、粗粒度测距技术。其基本原理是采用理论或经验模型将无线信号的传输损耗转换成节点间距离，常用的传播路径损耗模型有：自由空间传播模型、对数距离路径损耗模型、哈它模型以及对数—常态分布模型等。传感器节点的通信芯片（如 CC2431）通常提供测量接收强度的方法，可在接收数据分组的同时完成 RSSI 测量，无需配置额外硬件。并且 RSSI 测距的精度对于大多数定位应用已经足够，因此 RADAR 和 SpotON 等系统均采用 RSSI 测距技术。目前研究者也提出了许多校准技术，能有效减少 RSS 测距的误差，如高斯模型拟合[10]、片内多径分离技术[11]等。

由于信号强度比其他传播属性（如时延）更容易被外界干扰，因此 RSSI 测距相对其他测距技术更加脆弱。其测距结果不仅易受背景干扰、反射、多径传播和天线增益等环境或硬件因素的影响，而且很容易被攻击者采用重放和干扰等手段进行篡改。根据对测距的影响不同，可将针对 RSSI 的测距攻击分为两大类：虚增测距攻击和虚减测距攻击。由 RSSI 测距原理可知，削弱信号强度可虚增测距结果，反之则虚减测距结果。因此，虚增测距攻击的主要方式有：1）重放攻击，攻击者先阻塞原始信号，再以更低的功率重放，如图 1（a）所示；2）湮灭攻击，攻击者发送反相信号来湮灭原始信号或降低其强度，如图 1（b）所示；3）攻击者在

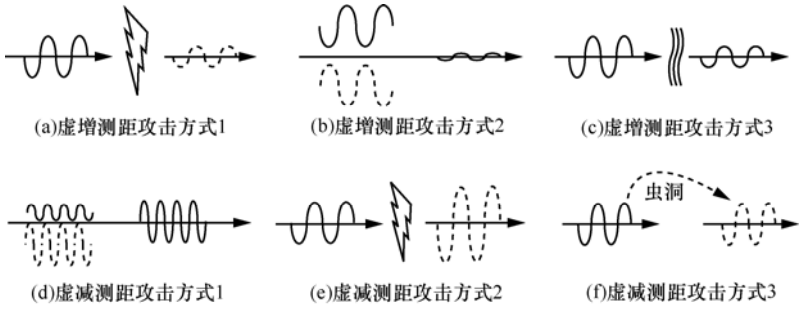


图 1 RSSI 测距攻击示意（虚线为攻击信号）

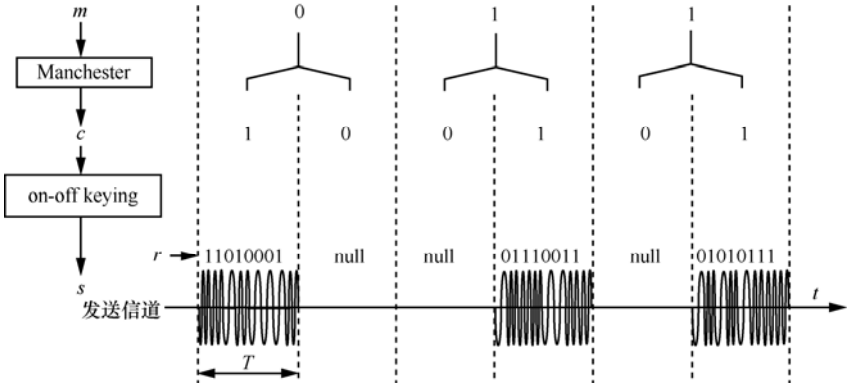


图 2　I-Codes 的编码示例（k=8）

信道中设置障碍物来削弱信号强度，如图 1（c）所示。虚减距离攻击的主要方式有：1）伪造插入，攻击者伪造并插入更强的信标信号来遮蔽原始信号，如图 1（d）所示；2）重放攻击，攻击者先阻塞原始信号，再以更高的功率进行重放，如图 1（e）所示；3）虫洞攻击，攻击者汇聚某区域的信标信号并通过虫洞重放到其他区域，如图 1（f）所示。此外，攻击者也可以进行全时段全频带的阻塞攻击。现有传感器节点一般采用 Chipcon 系列的 IEEE 802.15.4 或蓝牙等模块，其发射功率较低（<1mW），因此很容易遭受全频带阻塞攻击。

3　安全的 RSSI 测距协议

加密和认证等常规的安全机制都无法抵抗上述针对信标信号的攻击。本节中，提出了一种安全下界的 RSSI 测距协议，简称 S-RSSI。S-RSSI 采用完整性编码来同时保护数据和信号强度的完整性，不仅可以抵抗伪造插入、重放/虫洞等常规攻击，并且可防止信标信号被干扰而削弱。

3.1　完整性编码技术

完整性编码采用信号能量的有无来表示数据，并利用随机信号的不可湮灭性和曼彻斯特编码来防止数据被篡改。假定信标消息为 m，则 I-Codes 的编码过程为：1)对 m 曼彻斯特编码，即 c=Manchester(m)，规则为 1→“01”和 0→“10”，如 m=“0110”，可得 c=“10010110”；2) 对 c 进行基于随机信号的开—关键控调制，输出信号 s，即 s=on-off-keying(c)，规则为在 c 的每个码位周期 T 内，若 c_i=1 则输出随机信号，若 c_i=0 则保持信道空闲。现有传感器节点的无线模块一般无法直接输出随机信号，因此可通过以下方法来间接生成随机信号：首先生成一个 k 位的随机二进制序列 r，$r\in\{0,1\}^k$，再对 r 进行频移键控调制。节点的无线模块一般都支持频移键控调制，如 CC1000 在 300~1 000MHz 范围内可编程[12]。图 2 为上述 I-Codes 的一个示例。

I-Codes 的解码过程如下：1）接收方监听信道并测量每个 T_i 周期的平均信号接收强度，记为 $\overline{p_r(T_i)}$，如果 $\overline{p_r(T_i)}\geqslant p_t$，则 c_i=1，否则 c_i=0，从而获得码字 c，其中 p_t 为预设的强度门限；2）对 c 进行曼彻斯特解码，获得消息 m，并校验其完整性。关于信标帧的同步问题将在 4.2 节中进行讨论。

3.2　测距协议

S-RSSI 协议引入 I-Codes 编码来同时保护信标消息和信号强度的完整性，并采用不间断占用信道来防范伪造插入和重放攻击。适用 S-RSSI 的前提条件为：测距过程中，必须保证未知节点（待定位的节点）处于信标节点的信号覆盖范围内。传感器网络可以通过策略部署信标节点，以确保部署区域中每个未知节点都能处于若干信标节点的信号覆盖范围内。下面，以伪代码形式描述 S-RSSI 协议，如图 3 所示。

Secure RSSI ranging protocol
BN: Generate $m=\{BN, p_s\}$ and compute c=Manchester (m)
BN→*S*: On-off-keying (…111000||c||111000||c…) //不间断发送
S: Randomly receive a beacon(c) and record the max power $p_r^{\max}$ at which it is received.//随机接收一个信标帧，并统计其接收强度
Verify the integrity of c using I-codes，if c is valid then from p_s and $p_r^{\max}$ compute $D_{S\text{-}BN}$ else abort.

图 3　R-RSSI 测距协议

如图 3 所示，*BN* 表示信标节点，*S* 表示未知节点，“||”为消息连接符。在测距协议中，*BN* 首先产生测距报文 m，m 包含其 ID 和发射功率 p_s，并计算 m 的曼彻斯特码 c。在测距过程中，*BN* 采用 2.1 节所述的 on-off-keying 调制方法不间断发送 c（作

为信标帧），并插入定界符“111000”用于指示每个帧的起止。由于“111000”不是合法的曼彻斯特码字，因此不会出现在任何信标帧中。未知节点 S 从连续发送的信标帧中随机接收一个 c 作为测距信标，并测量其最大信号接收强度 $p_{\mathrm{r}}^{\max}$，$p_{\mathrm{r}}^{\max}=\max(\overline{p_r(T_i)})$，$i=1\cdots n$，$n$ 为 c 的码位数。最后，S 依据 I-Codes 规则校验接收到的 c 是否合法，并根据发射强度 p_s 和接收强度 $p_r^{\max}$ 计算出其到 BN 的距离 $D_{S\text{-}BN}$。

3.3 测距协议的安全性分析

3.3.1 接收强度的完整性分析

S-RSSI 是依据最大接收强度 $p_r^{\max}$ 来计算距离，因此攻击者可能通过插入干扰信号来改变信标的信号强度，从而篡改测距结果。如果攻击者选择在每个码位‘1’的信号周期内插入干扰信号，则这种策略性的干扰攻击并不会造成 c 编码违例，接收方无法通过曼彻斯特编码来检测攻击。下面，详细分析干扰信号对信标接收强度的影响情况。由于信标帧中的码位‘0’并不参与测距计算，因此下列分析均忽略之。

1) 单个时隙 T_k（$T_k=\dfrac{T}{k}$）的情形

假定在一个 T_k 时隙内，位于接收端的信标信号是一个频率为 f_0 的规格余弦波 $s(t)=\cos(\omega_0 t)$，$\omega_0=2\pi f_0$，并假设攻击者获知信标频率和振幅，则其发送的干扰信号可定义为 $s'(t)=A\cos(\omega_0 t+\theta)$，其中，$A$ 为振幅（$A>0$），θ为干扰信号与信标信号的相位差，$\theta\in[0,2\pi)$，则两者叠加后的接收信号可定义为 $r(t)=\cos(\omega_0 t)+A\cos(\omega_0 t+\theta)$，则 $r(t)$ 的平均能量 $\overline{E(T_k)}$ 可采用如下公式计算

$$\begin{aligned}\overline{E(T_k)}&=\frac{1}{T_k}\int_0^{T_k} r^2(t)\mathrm{d}t=\frac{1}{T_k}\int_0^{T_k}(\cos(\omega_0 t)+A\cos(\omega_0 t+\theta))^2\mathrm{d}t\\&=\frac{1}{T_k}\left(\frac{\sin(2\omega_0 T_k)}{4\omega_0}+\frac{T_k}{2}+A^2\frac{\sin(2\omega_0 T_k+2\theta)-\sin(2\theta)}{4\omega_0}+\right.\\&\left.\frac{T_k}{2}A^2+A\frac{\sin(2\omega_0 T_k+\theta)-\sin\theta}{2\omega_0}+AT_k\cos\theta\right)\\&\approx\frac{1}{2}+\frac{A^2}{2}+A\cos\theta\end{aligned}\tag{1}$$

由于传感器网络的通信频率一般比较高（如 f_0=5.0GHz），即$\omega_0=2\pi f_0>10^9$，且带宽较小（如 $S\leqslant$1Mbit/s），即 $\dfrac{1}{T_k}=s<10^6$；因此，式（1）中分母包含ω_0的分式都趋近于 0。图 4 为式（1）的函数示意图，其中参照线 E_0 为无攻击情况下的信号平均强度，即 $E_0=\dfrac{1}{T_k}\int_0^{T_k}\cos^2(\omega_0 t)\mathrm{d}t=0.5$。由图 4 可得，强度越大的干扰信号对信标接收强度的影响越大，位于参照线上的曲线表明该信号被增强了，而位于参照线以下曲线说明该信号被削弱了，其中信号被增强的情形占大部分。例如，当 A=1 时，仅当 $\theta\in\left[\dfrac{2\pi}{3},\dfrac{4\pi}{3}\right]$时，接收信号才会被攻击信号削弱；而当 A=2 时，任意θ的攻击信号均会增强信标。

由于 $\theta=2\pi f_0\dfrac{\Delta D}{C}$，其中，$\Delta D$ 为攻击者和信标节点分别到接收端的距离差，C 为光速。当信号频率较高时，细微的距离变化会导致显著的相位偏移，如当 f_0=5.0GHz 时，攻击者必须精确控制 $\Delta D\leqslant$ 6.7mm，才能确保攻击信号的 $\theta\in\left[\dfrac{2\pi}{3},\dfrac{4\pi}{3}\right]$。在实际环境中，攻击者很难实现如此高精度的攻击，并且多径反射和节点位移等不确定因素均对ΔD 有显著影响。因此，可以将攻击信号的θ看成是随机变量Θ的一个样本，$\Theta\sim U[0,2\pi)$。则攻击者至少将信号平均强度削弱了$(1-\alpha)\times100\%$的概率（$0\leqslant\alpha\leqslant1$），记为 $p_\alpha(T_k)$，可采用如下公式计算

$$\begin{aligned}p_\alpha(T_k)&=\mathrm{P}\left(\frac{\overline{E}_r}{E_0}\leqslant\alpha\right)=\mathrm{P}(1+A^2+2A\cos\theta\leqslant\alpha)\\&=\mathrm{P}\left(\cos\theta\leqslant\frac{\alpha-1-A^2}{2A}\right)\end{aligned}\tag{2}$$

令函数 $f(A)=\dfrac{\alpha-1-A^2}{2A}$，$A>0$。由于$f(A)$存在一阶导数，且$f'(A)=(\alpha-1)\times A^3<0$，因此$f(A)$为凸函数。由此可知，$f(A)$在 $f'(A)=0$ 处取最大值，即当 $A=\sqrt{1-\alpha}$ 时$f(A)$最大。则

$$\begin{aligned}p_a(T_k)&=\mathrm{P}\left(\cos\theta\leqslant\frac{\alpha-1-A^2}{2A}\right)\\&\leqslant\mathrm{P}(\cos\theta\leqslant-\sqrt{1-\alpha})\\&=\mathrm{P}(\theta\in[\theta_\alpha,2\pi-\theta_\alpha])=1-\frac{\theta_\alpha}{\pi},\\&\theta_\alpha=\arccos(-\sqrt{1-\alpha})\end{aligned}\tag{3}$$

2) 一个码位周期的情形

由于 I-Codes 采用了扩频技术，每个码位周期 T

可进一步划分成 k 个更小的时隙 T_k，发送方在每个 T_k 内均向无线信道发送一个相位在[0, 2π)内均匀分布的信号。因此，可将一个周期 T 的信标信号看成是一个由 k 个相位在[0,2π)内均匀分布的随机信号组成的随机过程，即 $c(t)=\cos(\omega_0 t+\Phi)$，其中 $\Phi\sim U[0,2\pi)$。假定一个门限 k_t，即如果一个 T 周期中有不少于 k_t 个时隙的信号被削弱了$(1-\alpha)\times100\%$，则该码位的平均强度将被削弱$(1-\alpha)\times100\%$。由于 Φ 与 Θ 相互独立，因此，对于同一个攻击者而言，每个时隙对应的 $p_\alpha(T_k)$都相同。则给定一个 T 周期的信标信号，令 $p=p_\alpha(T_k)=1-\frac{\theta_\alpha}{\pi}$，$q=1-p=\frac{\theta_\alpha}{\pi}$，则该信号被削弱$(1-\alpha)\times100\%$的概率 $p_\alpha(T)$，可采用如下二项分布公式计算

$$p_a(T)=\mathrm{P}(k_a\geqslant k_t)\leqslant\sum_{i=k_t}^{k}\binom{k}{i}p^i q^{k-i}$$

$$=\sum_{i=k_t}^{k}\binom{k}{i}\left(1-\frac{\theta_\alpha}{\pi}\right)^i\left(1-\frac{\theta_\alpha}{\pi}\right)^{k-i}\qquad(4)$$

图 5 为式（4）的函数示意图（不失一般性地假定 $k_t=\frac{k}{2}$）。从图 5 可得，$p_\alpha(T)$随着 k 增大而减小，且 α 越小则 $p_\alpha(T)$ 越小。例如，当 k=100 时，$p_{0.9}(T)$=0.024，$p_{0.8}(T)$= 0.001 7；当 k=200 时，$p_{0.9}(T)$=0.002 1，而 $p_{0.8}(T_k)\approx1.3\times10^{-5}$。由此可得：增大 k 值（即增大扩频系数），可提高信号强度下界的安全性，防止信号被削弱。但上述分析也表明攻击信号有可能会增强信标的接收强度，下一节将讨论虚减测距攻击的防范。

进一步分析 k_t 的取值。假定 c 中包含 n 个‘1’，则为了保证 S-RSSI 测距的安全性，门限 k_t 应满足条件：$p^n(k_a<k_t)\to1$。先假定一个ε值（$0\leqslant\varepsilon\leqslant1$），使得当 $P(k_\alpha<k_t)\geqslant(1-\varepsilon)$ 时，$P^n(k_\alpha<k_t)\geqslant(1-\varepsilon)^n\approx\mathrm{e}^{-n\varepsilon}\to1$。则给定一个 n，可以通过选择适当的ε值，使得 $P^n(k_\alpha<k_t)\to1$ 条件成立，从而获得 k_t 的取值约束

$$P(k_\alpha<k_t)=\sum_{i=1}^{k_t-1}\binom{k}{i}\left(1-\frac{\theta_\alpha}{\pi}\right)^i\left(\frac{\theta_\alpha}{\pi}\right)^{k-i}\geqslant(1-\varepsilon)$$

如当 n=1 000，可令ε=0.000 001，则 $\mathrm{e}^{-n\varepsilon}$=0.999 →1，使得 $P(k_a<k_t)\geqslant$0.999 999。图 6 为 $\frac{k_t}{k}$ 关于（k，α）的函数图。由图 6 可知：k 不能太小，否则 $\frac{k_t}{k}\to1$，即 $k_t\to k$。因此，可以根据给定的 n 值和 $\frac{k_t}{k}$ 的比例要求，来选择适当的 k 值。

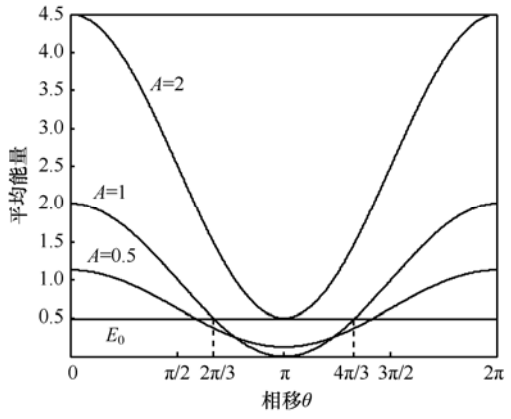


图 4　干扰信号对接收强度的影响

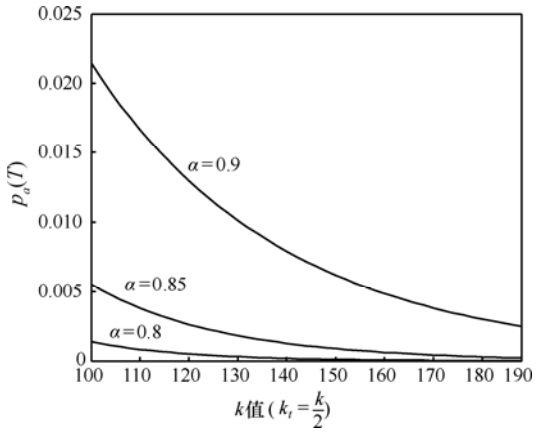


图 5　$p_\alpha(T_k)$的函数示意

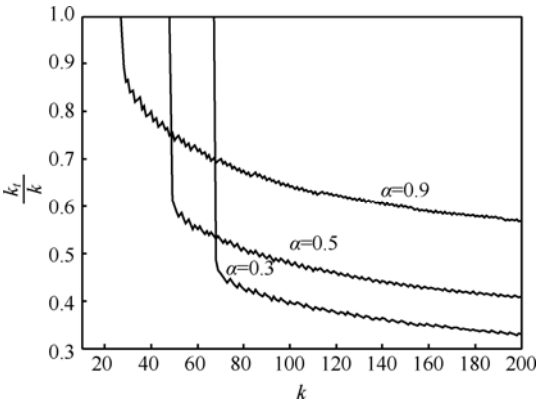


图 6　$\frac{k_t}{k}$ 关于 k 的函数关系（n=1 000）

3.3.2　防范其他外部攻击

在 S-RSSI 协议中，信标节点连续发送信标帧，从而不间断地占用无线信道。因此，攻击者实施伪造、重放和虫洞攻击所插入的信号必然与原始信号

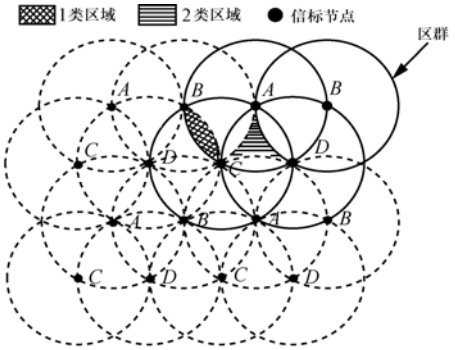
发生冲突。如果 2 个信号的相位不同，则这种叠加将导致接收消息中部分的“0”被篡改为“1”，从而产生编码违例。接收者可以通过检查数据是否编码违例来检测上述攻击。值得说明的是，由于重放攻击必然要消耗一定时间，如 motes 级的重放攻击至少要消耗 1ms[13]，而传感器节点的发送速率一般大于 10kbit/s（如 Mica2 的发送速率为 19.2kbit/s），因此 motes 级的重放信号至少与原始信号存在几十个数据位的相位差。

4　安全定位机制

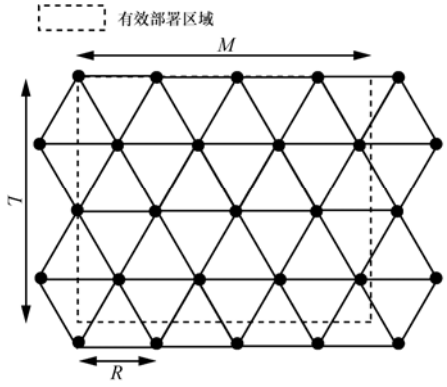
本节基于 S-RSSI 测距协议设计了一种安全的定位机制 SeRLA。SeRLA 采用基于蜂窝结构的时空隔离机制来解决信道复用与不间断占用之间的矛盾问题，并引入可校验的多边测量方法来滤除虚减测距的外部攻击。

4.1　信标节点的部署与信道分配

S-RSSI 协议要求信标节点不间断占用无线信道（防范外部攻击），但定位系统要求每个未知节点都能接收多个（不少于 3 个）信标节点的定位信标才能实现定位。因此，为了避免信标节点间的信号相互干扰，设计了一种蜂窝结构的时空隔离机制来实现信道复用。信标节点的部署方式如图 7（a）所示，在网络区域中按蜂窝结构部署信标节点，使得每个信标节点的信号覆盖范围刚好对应一个小区，每 4 个小区（A、B、C、D）形成一个复用区群。则网络中的每个未知节点至少处于 3 个信标节点的信号覆盖范围内。假定传感器网络的部署区域为一个 $L\times M$ 的矩形区域（M>L），如图 7（b）所示。则该网络需要信标节点的数量为 $N=\dfrac{\left\lceil\dfrac{2M}{R}+3\right\rceil\left\lceil\dfrac{2L}{\sqrt{3}R}+1\right\rceil}{2}$[14]，其中，$R$ 为通信半径。



(a) 信标信号的覆盖范围



(b) 信标节点数量

图 7　信标节点的部署

这些区群构成了信道的时空复用分配。如图 8 所示，在一个复用区群内，信道的时间域被划分成连续的时隙（slot），并依次轮流分配给 4 个小区（$slot_1\rightarrow A$，$slot_2\rightarrow B$，$slot_3\rightarrow C$，$slot_4\rightarrow D$，…），区群间保持同步工作。信标节点在每个分配时隙内发送一个信标帧，在其他时隙内保持无线电静默（表示为 NULL）。时隙长度等于一个信标帧的发送时间，则在一个分配周期内，1 类区域内的节点可收到 4 个信标帧，而 2 类区域内的节点可收到 3 个信标帧。

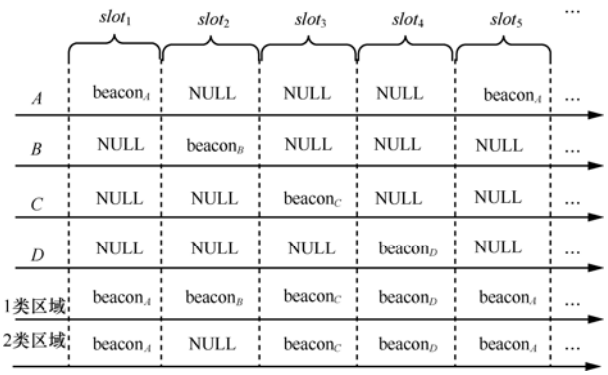


图 8　区群的信道时分复用示意

4.2　可校验的多边测量法

为了防范增强信号的攻击，采用一种类似于 VM 算法的可校验多边测量法 VLS（verifiable least squares estimate）。根据经典的回归理论，如果拟合结果适合于所给参照数据，则残差基本上可以反映误差的特性。反过来，如果测距误差的分布是已知，则通过分析残差可以检验所给参照数据是否服从假设的误差分布。利用这个规律可以检验定位参照集是否安全，即参照集中是否存在恶意攻击。VLS 算法如图 9 所示。

Verifiable Least Squares estimate
with all $l_i \in L$, compute the position (x_u', y_u') by LS
if for all $l_i \in L$, $\left|d_i - \sqrt{(x_i - x_u')^2 - (y_i \leqslant - y_u')^2}\right| \leqslant e_{\max}$
then $x_u = x_u', y_u = y_u'$
else the position is rejected

图 9　VLS 定位算法

如图 9 所示，$L=\{l_1, l_2, \cdots, l_n\}=\{(x_1, y_1, d_1), (x_2, y_2, d_2), \cdots (x_n, y_n, d_n)\}$，即信标节点提供的定位信息集合，$(x_i, y_i)$表示信标节点 i 的坐标，d_i 为未知节点与信标节点 i 之间的测量距离，$e_{\max}$ 为允许的最大测量误差，LS 为最小二乘法。

4.3　综合的安全定位算法 SeRLA

下面以一个区群为例，采用伪代码来描述 SeRLA 算法。SeRLA 算法包括三方参与者：4 个信标节点（a、b、c、d）、一个未知节点 s 和一个基站 sink。假定 s 位于区群的 1 类区域，则具体协议如图 10 所示。

SeRLA 算法包含 3 个环节：1）每个信标节点采用上述的信道复用机制和 I-Codes 机制不间断发送信标帧，如 $B_a=\{a, L_a, p_a^s\}$，其中，a 为信标节点的 ID，L_a 为 a 的位置坐标，p_a^s 为信号发送功率。“111000”用于指示每个信标帧的边界，NULL 表示无线电静默，则在信道中传输的数据流为“…111000||I-Code(B_a)||111000||I-Code(B_b)||111000||I-Code(B_c)||111000||I-Code(B_d)…”；2）未知节点 s 随机接收 4 个来自不同信标节点的信标帧（B_a, B_b, B_c, B_d），并记录每个信标帧的最大接收强度 p_x^r，然后向给基站报告一个采用共享密钥 ks 加密的定位报文；3）基站根据每个信标的发送和接收强度，分别计算出 s 和各信标节点的距离，然后采用 4.2 节所述的 VLS 算法估算出 s 的位置。由于信标节点不间断地发送信标，因此如果定位失败，未知节点可以重新执行 SeRLA 算法，直至成功。

4.4　定位安全分析

由 3.3 节可知，S-RSSI 测距不仅可以抵抗伪造插入、重放/虫洞等常规攻击，并且具有抵抗虚增测距攻击的能力。在此基础上，SeRLA 引入 VLS 算法进一步校验测距的一致性，通过分析残差可以检验所给参照数据是否服从假设的误差分布，滤除虚增测距的外部攻击。由于 RSSI 是一种粗粒度定位，恶意攻击只有显著篡改距离（超过 50%）才有意义，但这种显著攻击必然导致 VLS 校验失败。因此，SeRLA 定位机制能有效抵抗各种针对 RSSI 测距的外部攻击，且由于信标节点不间断地重复发送信标，未知节点可以重复执行 SeRLA，因此 SeRLA 定位机制也具有抵抗非全时段的阻塞攻击的能力。

但 4.1 节中的复用机制无法保证所有区域中的无线信道都会被信标信号填满，2 类区域中的信道存在空白时隙，因此攻击者仍有可能在该空白时隙内插入虚假信标消息。但是这种攻击只能在一定程度上影响 SeRLA。首先，攻击者只能攻击 2 类区域内的定位节点。如图 11 所示，在一个小区中，无空白时隙的区域面积为 $(4\pi - 6\sqrt{3})R^2$（阴影部分），其中，R 为通信半径，因此可能受攻击的区域只占 $1 - \dfrac{(4\pi - 6\sqrt{3})R^2}{\pi R^2} \approx 30\%$。其次，攻击者插入的非法

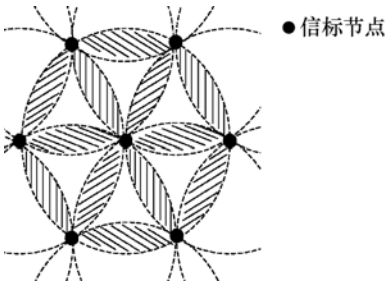


图 11　区群的信号覆盖情况

Secure RSSI-based Localization Algorithm
1)　a: …111000||I-code(B_a)||NULL||NULL||NULL…
　　b: …NULL||111000||I-code(B_b)||NULL||NULL…
　　c: …NULL||NULL||111000||I-code(B_c)||NULL…
　　d: …NULL||NULL||NULL||111000||I-code(B_d)…
2)　s: Verifies the integrity of B_a, B_b, B_c, B_d using I-codes.
　　: Record the max power levels at which Beacons are received .
$S \rightarrow sink$: $E_{ks}(B_a, B_b, B_c, B_d, p_a^r, p_b^r, p_c^r, p_d^r)$
3)　*Sink*: Extract $La, Lb, Lc, Ld, p_a^s, p_b^s, p_c^s, p_d^s, p_a^r, p_b^r, p_c^r, p_d^r$
　　: from $(p_a^s, p_b^s, p_c^s, p_d^s)$ and $(p_a^r, p_b^r, p_c^r, p_d^r)$, compute $(D_{a,s}, D_{b,s}, D_{c,s}, D_{d,s})$
　　: with $L_a, L_b, L_c, L_d, D_{a,s}, D_{b,s}, D_{c,s}, D_{d,s}$ computes the position of node s using VLS

图 10　SeRLA 定位算法

表 1　　文本方案与其他安全定位机制对比

安全定位机制	抵抗内部攻击	抵抗重放/虫洞攻击	抵抗信号攻击	定位精度	额外的硬件要求
VM、SecNav 等	是	是	是	高	纳秒级的时间测量精度和纳秒级的实时处理能力
AR-MMSE[5]、SecMCL[15]、LMS 定位等	是	是	是	高	节点需要执行复杂的计算，且良性参照必须超过半数
DV-Hop 的改进机制[16,17]	否	是	否	低	无
CBS[4]	是	否	否	高	隐蔽基站
Sec RSS[18]	否	是	否	中	精确的时间测量精度
本文方案	否	是	是	中	无

信标会导致测量距离和计算距离之间的差距超过门限 $e_{\max}$，从而被 VLS 所拒绝。

本文方案与其他安全定位机制的安全性能对比如表 1 所示。

5　结束语

本文提出一种适用于资源受限的传感器网络节点安全定位机制 SeRLA。与现有的节点安全定位方案相比，SeRLA 具有以下几个特点：1）低成本、低功耗，SeRLA 是基于 RSSI 测距，不要求节点配置额外的硬件设备（如超声波收发设备、实时运算单元和纳秒级精确测量装置等），也不需要传感器节点运行数字签名或顽健回归等复杂计算；2）SeRLA 采用单向广播的定位方式（类似 GPS），具有通信开销小、节点位置私密性高等优点；3）SeRLA 不需要传感器节点具有时间同步系统。

参考文献：

[1] CAPKUN S, HUBAUX J P. Secure positioning in wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):221-232.

[2] LAZOS L, POOVENDRAN R. SeRLoc: secure range-independent localization for wireless sensor networks[A]. Proc of the 2004 ACM Workshop on Wireless Security[C]. 2004. 21-30.

[3] ANJUM F, PANDEY S, AGRAWAL P. Secure localization in sensor networks using transmission range variation[A]. Proc of 2nd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems[C]. Washington, 2005. 195-203.

[4] CAPKUN S, CAGALJ M, *et al*. Secure localization with hidden and mobile base stations[A]. Proc of the 25th IEEE Conf on Computer Communications[C]. Washington, 2006. 23-29.

[5] LIU D, NING P, DU W K. Attack-resistant location estimation in sensor networks[A]. Proc of IPSN 2005[C]. Los Angeles, 2005. 99-106.

[6] LI Z, *et al*. Robust statistical methods for securing wireless localization in sensor networks[A]. Proc of IPSN 2005[C]. Los Angeles, 2005. 91-98.

[7] KAHN J M, KATZ R H, PISTER K S J. Next century challenges: mobile networking for “Smart Dust”[A]. Proc of the ACM MOBICOM[C]. 1999. 263-270.

[8] CAGALJ M, CAPKUN S, *et al*. Integrity (I) codes: message integrity protection and authentication over insecure channels[A]. Proc of the IEEE Symposium on Research in Security and Privacy[C]. Oakland, California, USA, 2006. 208-223.

[9] RASMUSSEN K B, *et al*. SecNav: secure broadcast localization and time synchronization in wireless networks[A]. Proc of ACM MobiCom[C]. 2007. 310-313.

[10] ZHANG J, ZHANG L. Research on distance measurement based on RSSI of ZigBee[A]. Proc Computing, Communication, Control, and Management[C]. 2009. 210-212.

[11] CLOSAS P, *et al*. A Bayesian approach to multipath mitigation in GNSS receivers[J]. IEEE Journal of Selected Topics in Signal Processing, 2009, 3(4): 695-706.

[12] Mica sensor platform[EB/OL]. http://www.xbow.com.

[13] GANERIWAL S, CAPKUN S, HAN S. Srivastava. secure time synchronization service for sensor networks[J]. ACM Transactions on Information and System Security (TISSEC), 2008, 11(4):1-35.

[14] ANJUM F, PANDEY S, AGRAWAL P. Secure localization in sensor networks using transmission range variation[A]. Proc of 2nd IEEE

（下转第 150 页）

based on high correlation of video sequences[A]. IEEE Internation Conference of Information and Technology[C]. 2010. 157-161.

[13] REN F, DONG J M. Fast and efficient intra mode selection for H.264/AVC[A]. IEEE, 2010 Second International Conference on Computer Modeling and Simulation[C]. 2010.202-205.

[14] 徐平，佘青山. 基于时空预测的 H.264 快速帧内预测模式选择算法[J]. 通信学报，2010，31 (9):139-145.
XU P, SHE Q S. New fast intra-prediction mode selection algorithm based on spatio-temporal predicting for H.264[J]. Journal on Communications, 2010，31 (9):139-145.

[15] 戴声奎，喻莉，朱光喜. 基于视频时空相关性的帧内预测模式抉择[J]. 通信学报，2005, 26(11):43-48.
DAI S K, YU L, ZHU G X. Intra-prediction mode decision based on video temporal and spatial correlation[J]. Journal on Communications, 2005, 26(11):43-48.

[16] 腾国伟，王国中. 一种基于自适应阈值的 H.264/AVC 帧内预侧快速模式选择算法[J].自动化学报，2006，32(4):526-533.
TENG G W, WANG G Z. A fast intra-prediction mode selection algorithm of H.264/AVC based on adaptive thresholds[J]. Acta Automatica Sinica, 2006，32(4):526-533.

[17] SHEN B, SETHI K. Direct feature extraction from compressed images[A]. Proceedings SPIE Storage & Retrieval for Image and Video Databases IV[C]. 1996. 2670-2676.

[18] 黄祥林, 沈兰荪. 基于 DCT 压缩域的图像纹理分类[J]. 电子与信息学报, 2002, 24(2): 216-221.
HUANG X L, SHEN L S. Texture-image classification in DCT compressed-domain[J]. Journal of Electronics and Information Technology, 2002, 24(2): 216-221.

[19] LEE S, KIM Y M. Fast scene change detection using direct feature extraction from MPEG compressed video[J]. IEEE Transactions on Multimedia, 2000,(4): 240-254.

作者简介：

詹舒波（1965-），男，江西广丰人，博士后，北京邮电大学教授、硕士生导师，主要研究方向为电信多媒体增值业务。

宋建斌（1977-），男，内蒙古呼和浩特人，博士，北京邮电大学博士后，主要研究方向为流媒体技术。

马丽（1978-），女，内蒙古鄂尔多斯人，硕士，北京联合大学讲师，主要研究方向为物流工程以及多媒体技术。

杨放春（1957-），男，北京人，博士，北京邮电大学教授、博士生导师，主要研究方向为计算机通信。

（上接第 142 页）

International Conference on Mobile Ad-hoc and Sensor Systems[C]. Washington, 2005. 195-203.

[15] ZENG Y, CAO J. SecMCL: a secure monte carlo localization algorithm for mobile sensor networks[A]. IEEE 6th International Conference on Digital Object Identifier[C]. 2009. 1054-1059.

[16] WU J, CHEN H, *et al.* Label-based DV-Hop localization against wormhole attacks in wireless sensor networks[A]. 2010 Fifth IEEE International Conference on Networking Architecture, and Storage[C]. 2010.

[17] CHEN H, LUO W, WANG Z. Secure localization against wormhole attacks using conflicting sets[A]. Proc of Performance Computing and Communications Conference , IEEE[C]. 2010.

[18] CAPKUN S, GANERIWAL S, ANJUM F, *et al*. Secure RSS-based Localization in Sensor Networks[R]. Technical Report 529, 2006.

作者简介：

叶阿勇（1977-），男，福建漳州人，博士，福建师范大学副教授、硕士生导师，主要研究方向为无线网络安全、无线定位安全等。

许力（1970-），男，福建福州人，博士，福建师范大学教授、博士生导师，主要研究方向为无线网络安全与性能优化。

林晖（1977-），男，福建南平人，福建师范大学博士生、讲师，主要研究方向为无线网络安全。