传感器节点定位系统攻防机制研究*)

曹晓梅[1,2] 何 欣[3] 陈贵海[2]

(南京邮电大学计算机学院 南京 210003)[1] (南京大学计算机软件新技术国家重点实验室 南京 210093)[2]

(西安交通大学计算机科学与技术系 西安 710049)[3]

摘 要 正确的节点位置信息是无线传感器网络许多功能模块实现的前提和基础,如网络构建和维护、监测事件定位、目标跟踪。在资源受限的传感器网络中,如何安全和有效地获取节点位置信息,是一个极具挑战性的安全问题。本文着重分析了不同的传感器节点定位系统所面临的各种攻击,分析了近年来该领域具有代表性的安全措施的原理、特点和局限,并简要介绍了该领域今后的研究热点。

关键词 无线传感器网络,节点定位系统,攻击,防御措施

Research on Sensor Node Localization Systems: Attacks and Countermeasures

CAO Xiao-mei[1,2] HE Xin[3] CHEN Gui-hai[2]

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[1]

(National Laboratory of Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]

(Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China)[3]

Abstract Correct node location information is the prerequisite and foundation of many wireless sensor network modules, such as network building and maintenance, monitoring event localization, and target tracking. In resource-constrained sensor networks, how to securely and effectively position sensor's coordinates is one of the most challenging security problems. This paper presents various attacks against different node localization systems, analyses the principles, characteristics, and limitations of recent representative secure localization countermeasures. Finally, the future research direction is summarized.

Keywords Wireless sensor network, Node localization systems, Attacks, Countermeasures

1 引言

无线传感器网络(本文简称传感器网络)可以实现复杂的大规模环境监测和目标追踪任务,在军事防备、环境监测、交通管理、灾难拯救等众多领域极具应用前景[1]。在传感器网络中,确定节点或事件发生的位置对其监测活动至关重要,其中节点自身的准确定位不仅是提供监测事件或目标位置信息的前提,也是提供网络拓扑自配置、提高路由效率、向部署者报告网络的覆盖质量以及为网络提供命名空间和位置敏感的安全模块等网络功能的基础[2]。

目前,已有许多系统和算法[3-10]致力于实现传感器节点的定位。然而,这些定位系统都假定安全可信的网络环境,忽略了定位过程中的安全问题。但是,传感器网络的开放性和无人看护性使节点的定位过程极易受到来自恶意节点或被俘获节点的攻击,例如无线信道干扰、伪造信标报文、节点移位和复制、虫洞攻击(wormhole attacks)、女巫攻击(sybil attacks)等。其中虫洞攻击指在两个相距较远的节点之间建立一个快速的无线电传输信道,使得这两个节点感觉彼此很接近;女巫攻击指一个恶意节点编造出许多不同身份,使得网络中出现多个不存在的节点,干扰定位协议的正常运作。攻击所产生的虚假位置信息将直接导致错误的监测结果,甚至使网络功能局部或整个瘫痪,进而给传感器网络应用,尤其是那些具有重要使命的应用(例如战场监视),造成难以估量的重大损失。因此,如何为存在敌对可能的传感器网络提供安全的节点定位系统是一个必须解决的关键问题。

从2003年开始,国外陆续有一些研究者致力于传感器节点定位系统安全性的研究[11-26],他们往往从不同角度入手,在安全目标、针对的定位技术和所采用的方法等方面有较大的差异,但彼此又存在一定的联系。本文旨在分析和比较不同定位技术所面临的攻击类型,深入探讨各种已提出的安全措施的实现原理、特点、局限和彼此的联系,并对相关领域的研究方向进行展望。

2 传感器节点定位系统简介

定位是指一个节点如何获取自己的地理位置信息。受价格、体积、功耗以及可扩展性等因素的限制,大多数传感器网络节点定位系统都采取利用信标节点辅助的节点定位方案,即网络中包含少量的信标节点(beacon node),这些节点通过携带GPS(Global Position System)定位组件等手段获得自身的位置信息,发送包含位置参照信息的信标报文,并建立坐标系。在未知节点的定位过程中,首先测量或估算未知节点与多个邻近信标节点的位置关系(距离、角度或区域包含关系

*)国家重点基础研究发展规划973(2006CB303000)、国家自然科学基金(60573131,60673154)、江苏省自然科学基金(BK2005208,BG2007039)。曹晓梅 讲师,博士研究生,主要研究无线网络安全;何 欣 讲师,博士研究生,主要研究网络计算和软件容错;陈贵海 教授,博士,主要研究领域为并行与分布式计算。

等),然后利用这些位置关系和特定算法计算出未知节点的坐标。执行计算的主体可以是未知节点、信标节点或者某个授权节点(authority),常用算法包括三边测量(trilateration)、三角测量(triangulation)或极大似然估计(multilateration)等。

根据是否实际测量节点间的位置关系,定位系统被分为基于测距(range-based)定位和无须测距(range-free)定位两类。基于测距定位需要测量节点间点到点的距离或角度信息,常用的测量技术有 TOA(Time of Arrival)[3],TDOA(Time Difference of Arrival)[4],AOA(Angle of Arrival)[5]和 RSSI(Received Signal Strength Indicator)[6]。无须测距定位利用网络连通性等信息估算节点间的位置关系,常用算法有质心算法(centroid algorithm)[7]、APIT 算法[8]、DV-Hop 算法[9]、Amorphous 算法[10]等,其中前两种算法通过邻居节点确定包含未知节点的区域,并把这个区域的质心作为未知节点的坐标;后两种算法均为基于距离向量(distance vector)的定位方法,即首先计算未知节点与信标节点间的最小跳数,然后信标节点估算平均每跳的距离,利用最小跳数乘以平均每跳距离,得到未知节点与信标节点之间的估计距离。

相比而言,基于测距定位借助超声波或无线射频信号的传输实际测量节点间的距离或角度,定位精度相对较高,但测量结果易受温度、湿度、障碍物等环境因素的影响;无须测距定位受环境因素的影响小,同时降低了对节点硬件的要求,更适合于大规模 WSN,但定位的误差有所增加。

3 节点定位系统所受攻击的分析

攻击者对传感器网络节点定位系统的攻击主要发生在位置关系的测量与估算阶段,攻击的目标通常是信标节点或者传输信标报文的无线链路,发起攻击的既可以是外部攻击者,也可以是被俘获的内部节点,恶意节点还可以相互协作发起攻击。针对节点定位系统的攻击具有两个显著特征:首先攻击目标具有明确的针对性,即为了提高破坏力,许多原有攻击被增强并侧重于信标节点和信标报文;其次攻击手段呈现多样性,即攻击的手段因系统所采用的定位技术和过程不同而异。

针对信标节点的攻击分为被动和主动两类,前者指攻击者通过移动、隔离信标节点降低定位精度,后者指攻击者通过俘获、假冒或复制信标节点发布虚假的信标报文,产生欺骗性的定位结果。针对信标报文传输过程的攻击与系统所采用的定位方案密切相关,具体分析如下:

• 针对基于测距定位的攻击

基于测距定位尤其容易受到发生在物理层或链路层的测距干扰或欺骗攻击,导致测距结果于实际结果的偏差超过正常范围。典型的攻击手段有:在测量接收节点和发射节点之间相对方位或角度的 AOA 算法中,通过设置反射物改变信号到达的角度;在利用理论或经验模型将传输损耗转化为距离的 RSSI 测距技术中,通过在信标节点与未知节点间设置具有吸收功能的障碍物,或局部提高周围信道噪声造成信号的衰减,使未知节点的测量距离长于实际距离;在利用测量呼叫-应答报文往返时间计算节点间距离的 TOA/TDOA 定位技术中,提前或者延迟发送响应报文以达到虚减或虚增节点距离的目的,等等。除此之外,攻击者还可以通过使用不同的传输介质或发射功率制造假象,导致错误的测量结果。

• 针对无须测距定位的攻击

类似地,无须测距定位在位置关系的估算阶段也容易受到以干扰或欺骗为目的的攻击,然而其种类不仅限于上述针对无线信道物理层或链路层的攻击,还包括针对网络层的攻击,如重放、伪造、篡改和丢弃信标报文,虫洞攻击,女巫攻击等。

具体来讲,在质心算法[11]中,未知节点确定自身位置为邻近 k 个信标节点所组成的多边形的质心:

$$(X_{est},Y_{est})=\left(\frac{X_1+\cdots+X_k}{k},\frac{Y_1+\cdots+Y_k}{k}\right) \quad (1)$$

其中 $(X_1,Y_1)\cdots(X_k,Y_k)$ 为未知节点能够接收到其信标分组的信标节点坐标。此时,攻击者可以通过隔离部分邻居节点(如在节点附近布置具有强吸收信号能力的障碍物等)降低判断精度。显然,邻近信标节点数量较少或分布不均,都会直接影响未知节点位置估计值的精确性。

在以 PIT(perfect point-in-triangulation test)理论为基础的无须测距定位(如 APIT 算法[8])中,假设在节点 M 的所有邻居节点中,相对于节点 M 没有同时远离或靠近三个信标节点 A,B,C,那么 M 就在△ABC 内,否则 M 在△ABC 外。攻击者可以发起针对 PIT 理论的虫洞攻击,如图 1 所示。

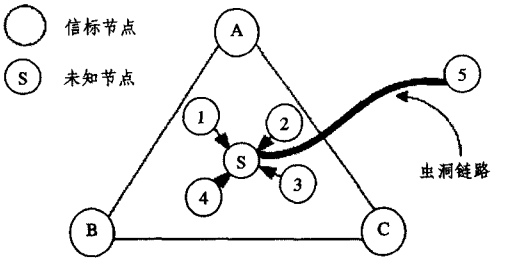

图 1 针对 APIT 算法的虫洞攻击

假定在节点 S 与节点 5 之间存在一条虫洞链路,而节点 5 同时远离三个信标节点,依据 PIT 原则,将得出 S 位于三角形之外的错误判断。

在基于距离向量的无须测距定位(如 DV-Hop 算法[9])中,攻击者可以通过直接移除节点导致每跳距离的计算误差,通过干扰或虫洞攻击诱导未知节点得到错误的距信标节点最小跳数值,使信标节点计算出错误的平均跳段距离。图 2 给出了针对基于距离向量的定位算法的网络层攻击:(a)是正常情况,(b)对应以减少跳数为目的的虫洞攻击,(c)对应以增加跳数为目的的干扰攻击。

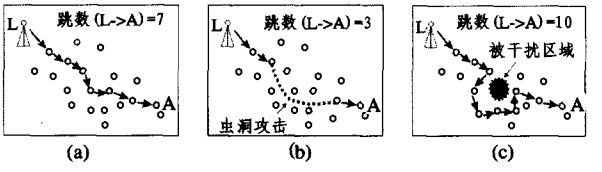

图 2 针对基于距离向量的定位算法的网络层攻击

表 1 对不同定位技术在通信过程中所面临的攻击种类进行了总结。

4 节点定位系统安全措施的分析与比较

常规安全机制,如抗泄密硬件/软件技术、扩频和编码技术以及对称和非对称加密算法等,难以防御上述针对不同定位技术物理属性或定位过程的脆弱性所发起的攻击,因此一些为传感器节点定位系统定制的安全措施[11-26]应运而生。根据安全目标不同,这些机制可以分为距离界定(distance

表1 针对不同定位技术的潜在攻击

定位技术	典型定位系统	攻击
TOA/TDOA	CRICKT	强制无线信号沿多径传输；提前或延迟发送响应报文；借助更快的介质传输信号
AOA	APS	强制无线信号沿多径传输；利用反射物改变信号到达角度；改变接收者的顺时针/逆时针方位
RSSI	RADAR	强制无线信号沿多径传输；引入不同微波或声波传输损耗模型；使用不同的功率传输信号；局部提升周围信道噪声
区域包围	APIT,SeRLoc	通过虫洞攻击扩大邻居范围；假造单跳距离；通过干扰改变邻居关系
距离向量	DV-Hop	通过虫洞攻击减小节点间路径长度；通过干扰增加节点间路径长度；通过改变无线电范围改变跳数；通过移除节点改变每跳距离
邻居节点位置	Centroid, SeRLoc	通过干扰减少无线电范围；通过虫洞或在更高能量上传输增大无线电范围；移动信标节点；改变天线接收模式

bounding)、安全定位与位置验证、入侵及异常检测与隔离，以及鲁棒性的节点定位算法等四个方面，不同协议或算法之间存在有较大的差异，但同时也有着一定的关联，在下面的内容中，我们将对此展开论述。

4.1 距离界定协议

距离界定最早由 Brands 和 Chaum 提出[27]，其基本思想是通过测量和计算验证者(verifier)与被验证者(claimant)之间距离的上界，防止以缩小测量/估算距离为目的的测距欺骗攻击，如虫洞攻击等。假定 v 是验证者节点，u 是被验证节点，该协议的伪代码如图3所示。需要说明的有以下几点：(1)报文的双向传输采用了无线射频信号(约 $3*10^8$m/s)，因此需要验证者具有纳秒级的时间测量能力，被验证者具有纳秒级的实时处理能力，对设备的硬件资源要求较高。(2) commit 函数通常是具有不可逆性和隐蔽性的单向哈希函数，前者指被验证者不能通过对 N_p 重新执行 commit 函数生成其他不同于(c,d)的二元组，后者表明仅获得二元组中的一个值 c 并不能得到 N_p，只有当全部获得二元(c,d)之后，通过执行 open 函数才能计算出 N_p 的值。二元组的计算、分时发送和验证过程可防止攻击者在协议执行过程中假冒被验证者的身份发送虚假的响应报文。(3)被验证者只有在完整地接收到验证者发送的包含随机现时值 N_v 的呼叫报文之后，才有可能得到正确的异或值并发回响应，从而防止被验证者提前发回响应报文。(4)呼叫与响应过程逐位操作，验证者计算每对传输时间的平均值作为最终的往返时间，使用该时间估算节点间距离，提高协议的健壮性。(5)被验证者发送的最后一条报文中包含了认证信息，其中 d 用于节点身份验证，MAC 值对报文的完整性进行验证。

为了减少对设备硬件的要求，Sastry 等在文献[27]的基础上，提出了适用于传感器网络的 Echo 协议[11]，其中呼叫报文仍采用无线射频信号发送，响应报文则通过超声波信号发送给验证者。由于超声波信号的传输速度相对较慢，因此对被验证者实时处理能力以及验证者时间测量能力的精确度要求有所降低；另外，报文的内容和传输方式也被简化，呼叫和响应报文中仅包含由验证者生成的现时值 N，报文作为整体被发送和接收，验证成功的必要条件之一就是两个报文中的现时值一致。为了防止攻击者假冒被验证者发回响应，文献[11]进一步提出了具有报文认证能力的变种 Echo 协议，该协议要求验证者与被验证者之间具有共享密钥 K 和预置的伪随机函数 F(如 AES,SHA1-MAC)，被验证者在收到呼叫报文之后计算并响应 $F_K(N)$，验证者收到该报文之后可以执行同样的计算，并判断结果是否与接收到的值相同，若相同则验证了节点的身份。变种 Echo 协议的不足之处在于往返时间中包含了加密算法的处理时间，即便这部分处理时间可以预先估计并在验证时被减去，仍然增加了协议的偶然性。最近，Meadows 等提出了一个类似于文献[27]的距离界定协议[12]，其主要贡献在于通过对协议的安全性进行形式化分析，实现了在保证同等安全性的同时，最小化报文和密码机制的复杂性。

```
u:          生成随机现时值 Nu
            计算二元组(c,d)=commit(Nu)
u ⟶  v:c
v:  生成随机现时值 Nv
v ⟶  u :Nv(从右向左逐位发送)
u ⟶ v:Nu ⊕ Nv(从左向右逐位发送)
v: 测量发送 Nv 到收到 Nu ⊕ Nv 所用的时间 tuv
u ⟶ v:Nu,Nv,d,MAC_Kuv(u,Nu,Nv,d)
v: 验证 MAC 以及 Nu=open(c,d)是否成立
```

图3 距离界定协议伪代码

Hancke 等提出了一种基于 RFID(Radio Frequency Identification)技术的距离界定协议[13]，协议假定验证者与被验证者具有共享认证密钥 K 和相同的伪随机函数 F，然而现时值 N 的发送和 $F_K(N)$ 的计算在计时开始之前完成，之后被验证者将 $F_K(N)$ 分为 $R^0||R^1$ 两个部分并分别置入不同的移位计算器，随后呼叫-响应过程开始：验证者首先生成一组随机位串并逐位发送给被验证者，被验证者根据所收到的位决定从哪个寄存器中取当前的首位作为响应；每发回一个响应，两个寄存器同时左移一位，当收到随机位串中最后一位得到响应之后，整个呼叫响应过程终止，最后验证者对收到的位串进行验证，若成功则取每对传输时间的平均值作为最终的往返时间。由于被验证者在收到呼叫报文到发送响应之间所需执行的操作仅是对两个寄存器中的值左移一位，因此优化了处理延迟。

需要指出的是，基于单个验证者的距离界定协议[11-13,27]只能得出节点间距离的上界，因而无法防止攻击者发起的以扩大测量距离为目的的攻击；另外，它们仅能验证节点是否位于指定区域内，不能验证节点是否在一个特定位置。为了解决这两个问题，引出了安全定位和基于多验证者的位置验证协议。

4.2 安全定位与位置验证协议

安全定位协议的目标是在存在攻击的情况下计算出节点的位置，而位置验证的目的是判断节点声称位置的准确性。根据所针对的定位系统不同，安全定位协议可以分为基于测距安全定位[14-17]与无须测距安全定位[18-21]两类。

Capkun 等提出了基于距离界定协议的 VM(Verifiable Multilateration)机制[14]，该机制借助一个授权节点和若干信标节点协作实现网络中未知节点的安全定位和对定位结果的验证。具体来讲，VM 假定未知节点 u 位于多个信标节点$(v_1,v_2,\cdots,v_n)$的传输半径内，每个信标节点 v_i 首先执行距离界定协议得到与 u 之间距离 $d_i(1\leqslant i\leqslant n)$，并将位置参照信息

$\{x_i, y_i, d_i\}$发送给授权节点，其中 x_i, y_i 为 v_i 的坐标；授权节点随后执行 LS(Least Squares)算法得到 u 的坐标$(\tilde{x}_u, \tilde{y}_u)$，LS算法表征如下：

$$(\tilde{x}_u, \tilde{y}_u) = \arg \min_{(x_u, y_u)} \sum_{i=1}^{n} [\sqrt{(x_i - x_u)^2 + (y_i - y_u)^2} - d_i]^2 \quad (2)$$

该算法使用使等式(1)右侧的求和表达式值最小的两元组作为未知节点坐标。在随后的位置验证阶段，授权节点验证每组$(x_i, y_i, , d_i)$与$(\tilde{x}_u, \tilde{y}_u)$之间的方差是否小于指定阈值，并且$(\tilde{x}_u, \tilde{y}_u)$是否位于区域内任意三个信标节点构成的三角形内，如果为真则接收$(\tilde{x}_u, \tilde{y}_u)$为节点的真实坐标，否则拒绝计算结果。根据 PIT 原理[8]，如果 u 虚增了与某个信标节点间的距离，为了保证一致性，该节点需要证明与其他两个信标节点中至少一个的距离小于实际的距离，这与距离界定协议相矛盾。因此，通过多个信标节点的合作，VM 机制成功地防止了距离扩大攻击。

Zhang 等提出了 SLS (Secure Localization Scheme) 方案[15]，该方案同样也利用了距离界定技术实现安全的节点定位，与 VM 不同之处有以下三点：首先，SLS 利用移动的信标节点取代静止的信标节点，以减少信标节点的数量；其次，每个信标节点 v_i 反复 K 次测量与某个未知节点之间的距离，并取中值作为 d_i；最后，负责收集位置参照信息、计算并验证节点位置的授权节点由信标节点轮流承担。相比 VM 而言，SLS 方案具有更高的鲁棒性和灵活性，但方案的复杂度和开销更高。

Capkun 等提出基于 CBS(Covert Base Station)的安全定位[16]。网络中包含少量 CBS，这些 CBS 可以是隐藏或伪装了的静态基站，也可以是随机移动的动态基站，它们使用有线介质或红外线与验证中心(verification authority)进行双向通信，其位置仅为验证中心所知。在基于 CBS 和 TDOA 算法的安全定位过程中，CBS 监听网络中公共基站(public base station)与传感器节点之间传输的信标报文，根据信标报文到达不同 CBS 的时间差估算节点的位置，随后对该位置进行验证。图 4 给出协议模型。

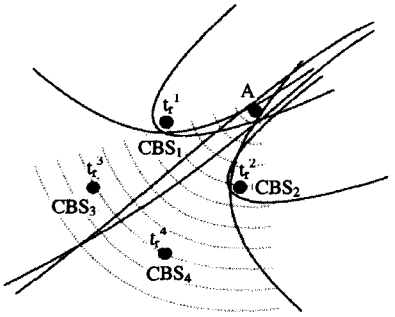

图 4　基于 TDOA 算法的 CBS 安全定位

其中 4 个 CBS 分别在不同时刻$(t_r^1, t_r^2, t_r^3, t_r^4)$收到传感器节点 A 的广播报文，之后验证中心执行 LS 算法得到 A 的坐标 p，LS 算法使用使等式(1)右侧的求和表达式值最小的 p^* 作为 A 的坐标：

$$p = \arg \min_{p^*} \sum_{i>j} (|t_r^i - t_r^j| - h(p^*, i, j))^2 \quad (3)$$

其中 $h(p^*, i, j)$表征 CBS_i 和 CBS_j 接收到从位置 p^* 发出的信号的时间差。基于 CBS 的定位方案通过多个 CBS 协作计算节点的位置并对该位置进行验证，由于攻击者无法精确预测所有 CBS 的位置，从而其欺骗性攻击难以奏效，进一步增加了定位系统的安全和鲁棒性；然而该方案依赖于 CBS 位置保密的较强假设，相关研究并不成熟。

Anjum 等提出了基于传输范围动态变动的 SLA (Secure Localization Algorithm) 算法[17]。SLA 假定每个传感器节点位于多个信标节点的覆盖范围之内，各信标节点每次使用不同的能量级安全的传输现时值，传感器节点将每个收到的现时值转发给 sink 节点，sink 节点根据这组从该传感器节点转发的现时值决定它的位置。与利用信号传输时间的安全定位方案[11-13,27]相比，SLA 不需要节点具有精确的时间测量和同步机制，降低了硬件要求。然而，SLA 假定不同的能量级别对应一定的传输半径，这种假设在室外环境是成立的，但针对室内环境的研究表明，给定的能量级别并不对应严格的传输范围[28]；另外，在 SLA 中所有节点位置的计算由 sink 节点集中进行，因此可扩展性较差。

Lazos 等针对无须测距定位系统分别提出了 SeRLoc 协议[18]、ROPE 协议[19]和 HiRLoc 协议[20]。SeRLoc 是一种完全分布式、局部化的安全定位协议，其设计目标是在非安全环境中，每个传感器节点借助少量可信信标节点的辅助正确地估算自己的坐标。该协议中，每个信标节点配置多个定向天线，信标报文中包含了节点天线发射角度，传感器节点根据接收到的来自多个信标节点的信标报文确定所在的最小交叉区域(minimum region of intersection)，最后通过质心算法确定自己的坐标。与此同时，SeRLoc 利用全局共享密钥和 RC5 算法加密所有信标报文，为报文通过机密性服务，采用单向哈希链(one-way hash chain)提供信标报文源端身份认证，每个信标报文的格式为：

$$L_i: \{(X_i, Y_i) || (\theta_1, \theta_2) || (H^{n-j}(PW_i)), j\} K_0 \quad (4)$$

其中 L_i 是信标节点的标识符，(X_i, Y_i) 是 L_i 的坐标，(θ_1, θ_2) 是 L_i 天线发射角度范围，$H^{n-j}(PW_i)$是用于提供信标节点身份认证的哈希链，PW_i 是 L_i 的密码，K_0 是网络共享密钥。借助定向天线的几何特性，SeRLoc 在假定没有恶意干扰的前提下可以检测出攻击者的虫洞攻击和女巫攻击。然而，SeRLoc 的不足之处在于：当攻击者利用选择性干扰破坏信标节点的传输时，将难以防止位置欺骗攻击；同时，为了获得最小交叉区域、提高定位精度，需要部署更多的信标节点或者为每个信标节点安装更多的定向天线。为了改进 SeRLoc 的不足，Lazos 等进一步提出了 ROPE 协议和 HiRLoc 协议。ROPE 协议在 SeRLoc 的基础上融入了距离界定技术，在不增加信标节点数量的情况下，尽可能减少选择性干扰、虫洞等诸多攻击对节点定位准确度的影响，然而该协议对节点的硬件提出了更高的要求，不仅需要具有多个定向天线的信标节点，而且所有节点必须具有纳秒级的时间同步系统和严格的实时处理能力，因此并不适用于低成本的传感器网络。在 HiRLoc 协议中，信标节点通过在其连续发送的信标节点中不断变换天线方向和传输范围，实现在不增加信标节点或定位天线的情况下减小最小交叉区域、提高定位精度，然而相比于 SeRLoc 协议，HiRLoc 增加了计算复杂度和通信开销。

Ekici 等提出了一种适用于高密度随机传感器网络的 PLV(Probabilistic Location Verification)算法[21]，该算法利用从源到目的的传输的广播报文在传输跳数和两点间欧几里得距离的概率性依赖关系，通过少量验证者协同确定声称位置的真实性概率以及可信等级。实验结果表明，当验证者的个数不小于 3 个时，算法具有较高的检测率和较低的误警率。算法的不足之处在于繁琐的计算给传感器节点和验证者节点带来较大的开销，并且算法难以检验出多个恶意节点协作发起的位置欺骗攻击，如虫洞攻击等。

4.3　入侵及异常检测与隔离技术

DoS(Denial of Service)攻击和利用被俘获节点发起的种

种攻击难以通过常规密码学机制防御，因此入侵及异常检测与隔离等反应式安全机制成为一个有力的补充，其目的在于尽可能减少 DoS 攻击、内部攻击等对定位系统的破坏。在传感器定位系统中，重点考虑的是对信标节点的入侵和异常检测与隔离。

Du 等给出了 LAD(Localization Anomaly Detection)方案[22]，检测在定位过程中异常的信标节点。该方案借助在许多传感器网络应用中可以事先获知的节点分布信息以及邻居节点间的组关系，检测节点的估计位置是否与它的观测位置一致。如果不一致的几率超过阈值，则 LAD 报告异常。模拟结果表明，异常的破坏程度越大，方案的误报率越低。然而，LAD 方案的检测准确率依赖于节点精确的分布概率信息，且该方案仅停留在对异常的检测，而没有给出如何处理异常，以及在发现异常之后如何提高定位正确性。

Liu 等给出了一组检测和移除被俘获的信标节点的技术[23]。在检测阶段，已知自己具体位置的信标节点彼此以未知节点的身份发送定位请求报文，使用响应报文中的信标节点坐标计算两点间的距离，并与测量距离比较，以判断误差是否在允许的范围之内。如果超过了预定阈值，则表明信标节点发送了虚假的坐标，此时向基站发送控诉报文。基站维护一个全局表，其中记录每一个信标节点被投诉的次数以及发送控诉报文的次数。当节点发送的控诉报文个数小于阈值 τ' 时，接受该节点发出的针对其他信标节点的控诉；当针对某信标节点的控诉数超过阈值 τ 时，该节点被基站撤销。相比于 LAD，该方案通过控诉和撤销机制将被俘获节点及时隔离在网络之外，提高了系统的鲁棒性。然而，由于采用了依赖基站的集中式控诉和撤销机制，导致基站成为了网络安全和性能的瓶颈点。

4.4 鲁棒性的节点定位算法

上述安全机制可以在一定程度上提高定位算法的安全性和可靠性，然而绝对的安全毕竟只是理论的概念，因此具有一定容攻击能力的定位算法成为当前的一个研究热点。由于具有较高的鲁棒性，基于统计分析的算法正被逐渐引入到 WSN 中，包括安全的节点定位[24-26]和安全的数据融合[29,30]等分支，为系统的可靠性和安全性提供了有力保障。

在传统的节点定位算法(如三边测量法、极大似然估计法)中，为了确定未知节点的坐标，首先需要获得一组邻近信标节点的位置参照信息，之后通过执行 LS 算法(参见公式(2))计算自身位置。然而，LS 算法的缺点在于容错性差[24]，即使是单个错误的位置参照信息也会对最终结果的正确性产生较大影响；因此 Li 等提出了基于 LMS (Least Median of Squares)的定位算法[24]，其目的是提高算法的鲁棒性，减少少量错误的位置参照信息对节点定位结果精度的影响。此时未知节点坐标 $(\tilde{x}_0,\tilde{y}_0)$ 为使公式(5)右侧表达式值最小的两元组：

$$(\tilde{x}_0,\tilde{y}_0)=\arg\min_{(x_0,y_0)} med_i\left[\sqrt{(x_i-x_0)^2+(y_i-y_0)^2}-d_i\right]^2 \quad (5)$$

其中 x_i，y_i 为信标节点 i 自身的坐标，d_i 为 i 到未知节点的距离。

Liu 等提出了一种 ARMMSE(Attack-Resistant Minimum Mean Square Estimate)算法[25]，利用最小方差中值的一致性特性(即表达式(2)右侧位置参照信息越不一致，相应的平均方差越大)，通过引入阈值和一种贪婪算法，对已知的所有位置参照迭代细分，判断并移除方差中值超过指定阈值的位置参照组，直到找到一组方差中值小于阈值的位置参照，或者发现迭代到组中位置参照的个数为 3 个时，仍然无法满足一致性要求。该算法通过隔离被俘获信标节点的错误位置信息，实现了定位算法的鲁棒性，然而由于算法对所有的位置参照进行迭代，因此计算复杂度较高。

为了提高计算效率，Wang 等引入数据挖掘中的聚类算法(cluster algorithms)，提出了 CMMSE(Cluster-based MMSE)[26]。协议在迭代之前，首先从所有位置参照中随机选取两个正确的位置参照作为种子，然后使用这两个种子逐个判断其余的位置参照与两者的一致性，检测结果分成两个集合：一致集(consistent set)和不一致集(non-consistent set)，最后对一致集中的位置参照信息进行迭代得到定位结果。显然，聚类的引入减少了迭代的轮数，提高了算法的执行效率。作者在一个由 MICAz 节点组成的实际测试环境中模拟和比较了 CMMSE，ARMMSE 和 LMS 算法，结果表明 CMMSE 在提供同等级别容错性的同时，计算速度最快。CMMSE 的执行效率依赖于正确种子参照的选取速度，如果网络中绝大多数信标节点是良性的，则两个正确的种子参照可以被很快的选取出来，之后只需一轮就可以从所有的位置参照中得到最大一致集；如果恶意信标节点数量较多，则计算时间延长，同时定位结果将产生较大误差。

结束语 在传感器网络中，传感器节点的位置信息至关重要，安全和准确地得到节点的位置信息是网络构建和维护、监测事件定位、目标跟踪等功能模块实现的前提和基础。近 3 年来，传感器网络节点定位系统的安全性研究进展可喜，取得了较为丰富的研究成果。本文在分析和比较不同类型节点定位系统所面临的安全攻击的同时，对已有的安全措施的实现原理、特点、局限和彼此的联系等相关工作进行了归纳和总结。

总的来说，传感器网络节点定位系统的各种安全措施在目标上互补，在实现上互相依赖。例如，在距离界定、位置验证等协议中，报文通过应用各种加密算法保证信息的完整性；一些安全定位协议[14,15]往往基于距离界定技术，并且在位置计算之后通过执行位置验证算法判断结果的真实性；入侵检测和隔离以及鲁棒性的节点定位算法作为常规安全机制的补充，减少了内部攻击对定位结果的影响，等等。从理论上来讲，一个完善的安全节点定位系统应该涵盖从常规安全机制到定制安全机制中的多个环节，然而任何一种安全措施都需要消耗一定的资源，包括节点自身的计算和能源开销，以及网络的通信开销等，因此需要综合考虑系统的应用背景、攻击模型、安全需求和资源条件等多种因素进行折中，以确定某个具体节点定位系统的防御策略。

随着传感器网络的不断发展和日益成熟，它将会被部署在更为特殊和复杂的应用环境中。移动网络环境下具有自调整性的安全定位算法或协议的实现将是一个热点研究方向。例如新兴的车载网络在优化交通流量、避免碰撞等方面极具应用前景，这类应用的共同特征是都涉及与生命安全相关的场景，车辆能否准确真实地定位，快速地进行位置验证，直接关系到车载网络能否提供正常服务，进而影响到事故的发生率[31]，因此如何实现快速变化环境中节点的安全定位是一个极具挑战性的研究课题。

参考文献

[1] 孙利民，李建中，陈渝，等. 无线传感器网络. 北京：清华大学出版社，2005

[2] 王福豹，史龙，任丰原. 无线传感器网络中的自身定位系统和算法. 软件学报，2005，16(5)：857-868

[3] Wellenhoff B H，Lichtenegger H，Collins J. Global positions sys-

tem: theory and practice [M]. Fourth Edition, Springer-Verlag, 1997
[4] Priyantha N, Chakraborty A, Balakrishnan H. The CRICKET location-support system [C]// Proc. of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM'00). Boston, MA, August 2000: 32-43
[5] Nicelescu D, Nath B. Ad hoc positioning (APS) using AOA. // Proc. of Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'03). San Francisco, CA, April 2003: 1734-1743
[6] Bahl P, Padmanabhan V N. RADAR: An in-building RF-based user location and tracking system [C]// Proc. of Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00). Tel Aviv, Israel, March 2000: 775-784
[7] Bulusun N, Heidemann J, Estr I D. GPS-less low cost outdoor localization for very small devices [J]. IEEE Personal Communications, 2000, 7 (5): 28-34
[8] He T, Huang C, Blum B M, et al. Range-free localization schemes in large scale sensor networks [C]// Proc. of the 9th Annual International Conference on Mobile Computing and Networking (MOBICOM'03). San Diego, CA, August 2003: 81-95
[9] Niculescu D, Nath B. DV-based positioning in ad hoc networks [J]. Journal of Telecommunication Systems, 2003, 22 (1/4): 267-280
[10] Nagpal R, Shrobe H, Bachrach J. Organizing a global coordinate system from local information on an ad hoc sensor network [C]// Proc. of the 2nd International Worksho Pon Information Processing in Sensor Networks (IPSN'03). Palo Alto, California, April 2003: 151-152
[11] Sastry N, Shankar U, Wagner D. Secure verification of location claims [C]// Proc. of the 2003 ACM Worksho Pon Wireless Security (WISE'03). San diego, California, September 2003: 1-10
[12] Meadows C, Syverson P, Chang L W. Towards more efficient distance bounding protocols [C]// Proc. the Second International Conference on Security and Privacy in Communication Networks (SecureComm'06). Baltimore, MD, August 2006: 1-5
[13] Hancke G P, Kuhn M G. An RFID distance bounding protocol [C]// Proc. of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05). Athens, Greece, September 2005: 67-73
[14] Capkun S, Hubaux J P. Secure positioning of wireless devices with application to sensor networks [C]// Proc. of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05). Miami, Florida, March 2005: 1917-1928
[15] Zhang Y, Liu W, Fang Y, et al. Secure localization and authentication in ultra-wideband sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(4): 829-835
[16] Capkun S, Cagalj M, Srivastava M. Secure Localization with Hidden and Mobile Base Stations [C]// Proc. of the 25th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'06). Barcelona, Spain, April 2006: 23-29
[17] Anjum F, Pandey S, Agrawal P. Secure localization in SN using transmission range variation [C]// Proc. of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS'05). Washington, DC, November 2005
[18] Lazos L, Poovendran R. SeRLoc: Secure range-independent localization for wireless sensor networks [C]// Proc. of the 2004 ACM Worksho Pon Wireless Security (WISE'04). Brisbane, Australia, November 2004: 21-30
[19] Lazos L, Poovendran R, Capkun S. ROPE: Robust position estimation in wireless sensor networks [C]// Proc. of the International Symposium on Information Processing in Sensor Networks (IPSN'05). Los Angeles, CA, April 2005: 324-331
[20] Lazos L, Poovendran R. HiRLoc: High-resolution robust localization for wireless sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 233-246
[21] Ekici E, Vural S, McNair J, et al. Secure probabilistic location verification in randomly deployed wireless sensor networks [J]. Ad Hoc Networks, 2007
[22] Du W L, Fang L, Ning P. LAD: Localization anomaly detection for wireless sensor networks [J]. The Journal of Parallel and Distributed Computing, 2006, 66(7): 874-886
[23] Liu D G, Ning P, Du W L. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks [C]// Proc. of the 25th International Conference on Distributed Computing Systems (ICDCS'05). Columbus, Ohio, June 2005: 609-691
[24] Li Z, Trappe W, Zhang Y, et al. Robust statistical methods for securing wireless localization in sensor networks [C]// Proc. of the International Symposium on Information Processing in Sensor Networks (IPSN'05). Washington, 2005: 91-98
[25] Liu D G, Ning P, Du W L. Attack-resistant location estimation in sensor networks [C]// Proc. of the International Conference on Information Processing in Sensor Networks (IPSN'05). Los Angeles, CA, April 2005. 99-106
[26] Wang C, Liu A, Ning P. Cluster-based minimum mean square estimation for secure and resilient localization in wireless sensor networks [C]// Proc. of the International Conference on Wireless Algorithms, Systems and Applications (WASA '07). Chicago, IL, August 2007
[27] Brands S, Chaum D. Distance-bounding protocols [C]// Proc. of Workshop on the theory and application of cryptographic techniques on Advances in cryptology. New York, 1994: 344-359
[28] Ganu S, Krishnakumar A S, Krishnan P. Infrastructure-based location estimation in wlan networks [C]// Proc. of IEEE Wireless Communications and Networking Conference (WCNC'04). Los Alamitos, 2004: 465-470
[29] Przyatek B, Song D, Perrig A. SIA: Secure information aggregation in sensor networks [C]// Proc. of the 1st International Conference on Embedded Networked Sensor Systems (SenSys'03). Los Angeles, CA, November 2003: 255-265
[30] Wagner D. Resilient aggregation in sensor networks [C]// Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04). Washington DC, Octobor 2004: 78-87
[31] Raya M, Hubaux J P. The security of vehicular ad hoc networks [C]// Proc. of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks (SASN'05). Alexandria, Virginia, November 2005: 11-21

(上接第 31 页)

BGP4 以及 BGP4+协议及其功能，介绍了相关的各种数据包功能，基于协议的说明生成了它的 IOFSM，基于已有算法自动生成了 10 个互操作性测试套。我们对现有的三个 BGP4+协议实现进行了互操作性测试，发现了一些不可互操作的地方，本项工作有利于检查产品的互联互通互操作能力。本文的实践结果可以为协议标准的设计提供合理的建议，减少说明中影响互操作性测试因素的存在。如果将互操作性测试方法用在协议开发的早期，可以增强产品的互操作能力。下一步的研究工作针对多激励原则展开互操作性测试，即从外界环境中可以同时向两个实现输入外部消息。这种原则要比单激励原则更加复杂，同时也需要研究新的形式化建模方法和测试套自动生成的算法，从而适用新的工作环境。

参 考 文 献

[1] Bates T, Rekhter Y, Chandra R. Multiprotocol Extensions for BGP-4 (BGP4+). RFC 2858, June 2000
[2] http://www.tahi.org
[3] http://www.unh.edu
[4] http://www.etsi.org
[5] Rekhter Y, LI T. A Border Gateway Protocol 4 (BGP-4). RFC 1771, March1995
[6] Rekhter Y, Li T, Hares S. A Border Gateway Protocol 4 (BGP-4). RFC 4271, January 2006
[7] 张涛. 边界网关协议 BGP4+的互操作性测试研究. 内蒙古大学, 2007
[8] Seol S, Kim M, Kang S, et al. Fully automated interoperability test suite derivation for communication protocols. Computer Networks, 2003, 43(6): 735-759