ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.4, April 2008, pp.879–887
DOI: 10.3724/SP.J.1001.2008.00879
© 2008 by *Journal of Software*. All rights reserved.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

传感器网络节点定位系统安全性分析*

曹晓梅[1,2+], 俞 波[3], 陈贵海[1], 任丰原[4]

[1](南京大学 计算机软件新技术国家重点实验室,江苏 南京 210093)
[2](南京邮电大学 计算机学院,江苏 南京 210003)
[3](复旦大学 计算机科学与工程系,上海 200433)
[4](清华大学 计算机科学与技术系,北京 100084)

Security Analysis on Node Localization Systems of Wireless Sensor Networks

CAO Xiao-Mei[1,2+], YU Bo[3], CHEN Gui-Hai[1], REN Feng-Yuan[4]

[1](National Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)
[2](College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)
[3](Department of Computer Science and Engineering, Fudan University, Shanghai 200433, China)
[4](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)
+ Corresponding author: Phn: +86-25-86473659, E-mail: caoxm@njupt.edu.cn, http://cs.nju.edu.cn/gap/cao/

Cao XM, Yu B, Chen GH, Ren FY. Security analysis on node localization systems of wireless sensor networks. *Journal of Software*, 2008,19(4):879–887. http://www.jos.org.cn/1000-9825/19/879.htm

Abstract: Correct node position information is the prerequisite and foundation of many sensor network modules, such as network building and maintenance, monitoring event localization, and target tracking. The node localization process is vulnerable to diverse attacks. In resource-constrained sensor networks, how to securely and effectively locate 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, future research direction is summarized.
Key words: wireless sensor network; node localization system; attacks; countermeasure

摘 要: 正确的节点位置信息是传感器网络构建和维护、监测事件定位、目标跟踪等模块实现的前提和基础.节点的定位过程极易受到各种攻击,在资源受限的传感器网络中,如何安全、有效地获取节点位置信息,是一个极具挑战性的安全问题.着重分析了不同类型的传感器网络节点定位系统所面临的安全攻击,讨论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
中图法分类号: TP393 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant Nos.60573131, 60673154, 60721002 (国家自然科学基金); the National Basic Research Program of China under Grant No.2006CB303000 (国家重点基础研究发展计划(973)); the Jiangsu High-Tech Research Project of China under Grant No.BK2007039 (江苏省高技术研究项目)
Received 2007-02-28; Accepted 2007-10-12

© 中国科学院软件研究所 http://www.jos.org.cn

无线传感器网络(wireless sensor networks)是由部署在监测区域内的大量微型、低成本、低功耗的传感器节点组成的多跳无线网络,实现监测区域内敏感数据的采集、处理和传输.作为连接物理世界和数字世界的桥梁,传感器网络在国防军事、环境监测、交通管理等众多领域极具应用前景,成为近几年国内外研究的热点[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等网络功能的基础[2].

绝大多数已有的传感器网络节点定位系统[3−10]均假定安全可信的网络环境,忽略了定位过程中的安全问题.然而,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.针对节点定位系统的攻击具有明确的针对性,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(beacon node)和信标报文;同时,攻击手段因系统所采用的定位技术和过程不同而有所不同,种类较多.攻击所产生的无效或错误的定位结果将可能导致严重后果(如错误甚至截然相反的监测结果、网络功能局部或整个瘫痪等等),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应用提供安全的节点定位系统,是一个必须解决的关键问题.本文旨在分析和比较不同定位技术所面临的攻击种类,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加以展望.

1 传感器网络节点定位系统

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,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(authority)节点,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.

定位系统包括基于测距(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),TDOA(time difference of arrival),AOA(angle of arrival)和 RSSI(received signal strength indicator).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、APIT 算法、DV-Hop 算法、Amorphous 算法等.

2 节点定位系统所受攻击的分析

攻击者对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.由于不同的定位系统基于不同的物理属性和定位过程,因此,攻击手段与系统所采用的定位技术密切相关,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,导致测距结果与实际结果的偏差超过正常范围.攻击者不仅可以移动、隔离信标节点降低定位精度,还可以发起无线电干扰攻击.例如,在发送者和接收者之间放置障碍物使信标报文沿多径传输,延长信号的传输时间、改变信号的到达角度或强度;在利用测量呼叫-应答报文往返时间计算节点间距离的TOA[3]/TDOA[4]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;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[5]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[6]中,通过在信标节点与未知节点之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.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

© 中国科学院软件研究所 http://www.jos.org.cn

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,其种类除了上述针对节点和无线信道物理层或链路层的攻击以外,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(sybil attack)等.其中,针对定位系统的女巫攻击是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.

具体来讲,在质心算法[7]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:

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

其中,(X_i,Y_i),$1\le i\le k$为信标节点坐标.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.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.

PIT(perfect point-in-triangulation test)理论假设在节点M的所有邻居节点中,相对于节点M没有同时远离或靠近 3 个信标节点A,B,C,那么,M就在$\triangle ABC$内,否则,M在$\triangle ABC$外.在以PIT理论为基础的APIT(approximate point-in-triangulation test)算法[8]中,攻击者可以发起虫洞攻击,如图 1 所示.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 3 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.

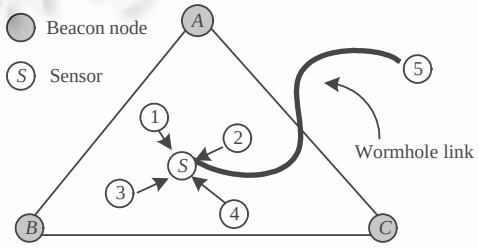
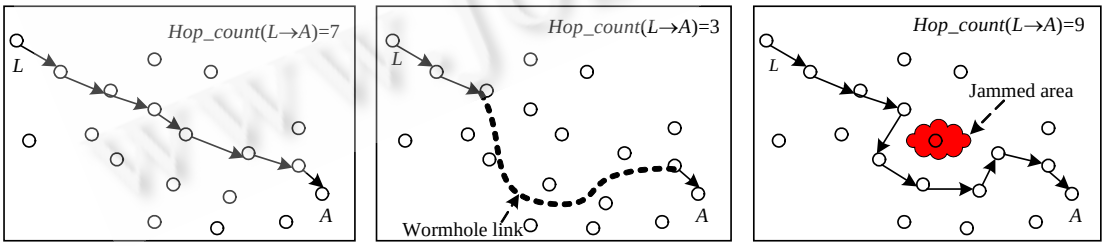


Fig.1 Wormhole attack towards APIT algorithm

图 1 针对 APIT 算法的虫洞攻击

在基于距离向量的无须测距定位[9,10]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的跳数值,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:图 2(a)是正常情况,图 2(b)对应以减少跳数为目的的虫洞攻击,图 2(c)对应以增加跳数为目的的干扰攻击.



(a) (b) (c)

Fig.2 Network-Layer attacks towards distance-vector based localization algorithms

图 2 针对基于距离向量的定位算法的网络层攻击

3 传感器网络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

© 中国科学院软件研究所 http://www.jos.org.cn

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应运而生.根据安全目标的不同,这些安全措施可以分为距离界定[11−13]、安全定位[14−21]、入侵及异常检测与隔离[22,23]以及鲁棒性的节点定位算法[24,25]4 个方面.不同协议或算法之间存在有着较大的差异,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.

3.1 距离界定协议

距离界定协议通过限定节点间距离的上界,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.Brands和Chaum最早提出时间绑定呼叫-响应协议(time-bounded challenge-response protocol)[11],测量和计算验证者(verifier)与被验证者(claimant)之间距离的上界.

假定 v 是验证者节点,u 是被验证者节点,该协议的伪代码如图 3 所示,需要说明的有以下几点:

(1) *commit*函数通常是具有不可逆性和隐蔽性的单向哈希函数,前者是指被验证者不能通过对N_u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_u,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_u的值,从而防止了攻击者在协议执行过程中假冒被验证者的身份发送虚假响应报文;

(2) 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,从而防止了被验证者提前发回响应报文;

(3) 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,提高了协议的健壮性;

(4) 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(message authentication code)值对报文的完整性进行验证,防止了攻击者篡改报文内容.

u: Generate random nonce N_u
Generate $commitment(c,d) = commit(N_u)$
$u \rightarrow v: c$
v: Generate random nonce N_v
$v \rightarrow u: N_v$ (bits sent from MSB to LSB)
$u \rightarrow v: N_u \oplus N_v$ (bits sent from LSB to MSB)
v: Measure time t_{uv} between sending N_v and receiving $N_u \oplus N_v$
$u \rightarrow v: N_u, N_v, d, MAC_{K_{uv}}(u, N_u, N_v, d)$
v: Verify MAC and verify if $N_u = open(c,d)$

Fig.3 Pseudocode of the distance bounding protocol

图 3 距离界定协议伪代码

由于协议在验证者和被验证者之间报文的双向传输中同时采用了无线射频信号(约 3×10^8m/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(在时间上,1 纳秒的偏差会导致 30cm 左右的测距误差[15]).研究表明,当前仅有少量技术(如UWB(ultra-wide band)[26])能达到这种精度.为了减少对设备硬件的要求, Sastry等人提出了适用于传感器网络的Echo协议[12],与文献[11]的主要区别是呼叫报文利用无线射频技术发送给被验证者,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的能力以及验证者时间测量能力的精确度要求有所降低.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,即使这部分处理时间可以预先估计并在验证时被减去,也仍然增加了协议的偶然性.近期,Meadows等人提出了一个类似于文献[11]的距离界定协议[13],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.

需要指出的是,基于单个验证者的距离界定协议[11−13]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

© 中国科学院软件研究所 http://www.jos.org.cn

定位置.为了解决这两个问题,引出了基于多验证者的安全定位和位置验证协议.

3.2 安全定位机制

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,根据所针对的定位系统的不同,分为基于测距安全定位[14−17]和无须测距安全定位[18−21]两类.

3.2.1 基于测距的安全定位机制

Capkun等人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($v_1,v_2,\ldots,v_n$)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之间的距离d_i($1\le i\le n$),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:

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

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 3 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等人提出了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机制的不同之处有以下 3 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.与VM相比,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等人提出基于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,每个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,并将估算结果发送给验证中心,由验证中心对该位置进行验证.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等人提出了基于传输范围动态变动的安全定位算法SLA(secure localization algorithm)[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[14−16]相比,SLA不需要节点具有精确的时间测量和同步机制.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[26].另外,在文献[14−16]中,节点位置的估算均由邻近的验证者实现,但在SLA中,所有节点位置的计算则由sink节点集中进行,因此可扩展性较差.

3.2.2 无须测距的安全定位机制

Lazos等人针对无须测距定位系统分别提出了SeRLoc协议、ROPE(robust position estimation)协议和HiRLoc协议.SeRLoc[18]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

© 中国科学院软件研究所 http://www.jos.org.cn

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

$$L_i:\{(X_i,Y_i)\|(\theta_1,\theta_2)\|(H^{n-j}(PW_i)),j\}K_0 \tag{3}$$

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,SeRLoc协议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等人进一步提出了ROPE协议和HiRLoc协议.

ROPE协议[19]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,尽可能地减少选择性干扰、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[20]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等人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传输的广播报文在传输跳数和两点间欧几里德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.同时,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.

3.3 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.在传感器网络定位系统中,重点考虑信标节点的入侵和异常检测与隔离.

Du等人给出了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相一致,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,越容易被检测出来,且误报率越低.然而,LAD方案依赖于节点的分布信息,因此,如果无法获得精确的分布概率,那么LAD的检测结果将受到极大的影响.同时,该方案仅停留在对异常的检测阶段,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等人给出了一组检测和移除被俘获的信标节点技术[23].在恶意信标报文的检测阶段,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信标节点位置信息.此外,文献[23]引入虫洞检测器(wormhole detector)验证报文的计算距离是否大于目标节点的信号传输范围:如果是,则表明信标报文通过虫洞链路被重放;否则,需要进一步通过验证检测到的节点间信标报文的RTT(round trip time)是否超过实际应有的时间,以过滤来自邻居节点的重放信标信号.每一个信标节点都可以向基站发送针对被怀疑节点的控诉报文.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.文献[23]的分析和模拟表明,当恶意节点数量较少时,这些技术能够有效地检测出网络中的恶意信标节点;然而,当网络中恶意节点的数量较多时,就会出现比较高的误报率(当网络中有 10 个恶意节点时,误报率将超过 20%).而且,由于采用了依赖基站的集中式控诉

© 中国科学院软件研究所 http://www.jos.org.cn

和撤销机制.因此,基站将成为网络性能和安全性的瓶颈点,完全分布式节点撤销机制的研究是一个有待解决的问题.

3.4 鲁棒性的节点定位算法

通过上述安全机制,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传感器网络中,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等人提出了基于LMS(least median of squares)的定位算法[24],其目的在于提高算法的鲁棒性,减少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 $(\tilde{x}_u,\tilde{y}_u)$ 为使公式(4)右侧表达式值最小的两元组:

$$(\tilde{x}_0,\tilde{y}_0)=\arg\min_{(x_0,y_0)} med_i[\sqrt{(x_i-x_0)^2+(y_i-y_0)^2}-d_i]^2 \tag{4}$$

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等人提出了一种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.

4 总结与展望

在传感器网络中,安全和准确地得到节点的位置信息是网络构建、维护、应用等功能模块实现的前提和基础.本文分析和比较了不同定位技术所面临的攻击种类,深入探讨了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.总之,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、安全定位机制中,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.

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[27].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.

References:

[1] Ren FY, Huang HN, Lin C. Wireless sensor networks. Journal of Software, 2003,14(7):1282−1291 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1282.htm

[2] Wang FB, Shi L, Ren FY. Self-Localization systems and algorithms for wireless sensor networks. Journal of Software, 2005,16(5): 857−868 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/857.htm

[3] Harter A, Hopper A, Steggles P, Ward A, Webster P. The anatomy of a context-aware application. In: Kodesh H, Imielinski T, Steenstrup M, eds. Proc. of the 5th Annual Int’l Conf. on Mobile Computing and Networking (MOBICOM). Seattle: ACM Press, 1999. 59−68.

[4] Priyantha N, Chakraborty A, Balakrishnan H. The CRICKET location-support system. In: Steere DC, Baptista A, Pu C, Walpole J, eds. Proc. of the 6th Annual Int’l Conf. on Mobile Computing and Networking (MOBICOM). New York: ACM Press, 2000. 32−43.

© 中国科学院软件研究所 http://www.jos.org.cn

[5] Nicelescu D, Nath B. Ad hoc positioning (APS) using AOA. In: Bauer F, Roberts J, Shroff N, eds. Proc. of the Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM). New York: IEEE Press, 2003. 1734−1743.

[6] Bahl P, Padmanabhan VN. RADAR: An in-building RF-based user location and tracking system. In: Sidi M, Sengupta B, eds. Proc. of the Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM). New York: IEEE Press, 2000. 775−784.

[7] Bulusun N, Heidemann J, Estr ID. GPS-Less low cost outdoor localization for very small devices. IEEE Personal Communications, 2000,7(5):28−34.

[8] He T, Huang C, Blum BM, Stankovic JA, Abdelzaher T. Range-Free localization schemes in large scale sensor networks. In: Johnson DB, Joseph AD, Vaidya NH, eds. Proc. of the 9th Annual Int'l Conf. on Mobile Computing and Networking (MOBICOM). New York: ACM Press, 2003. 81−95.

[9] Niculescu D, Nath B. DV based positioning in ad hoc networks. 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. In: Zhao F, Guibas LJ, eds. Proc. of the 2nd Int'l Workshop on Information Processing in Sensor Networks (IPSN). New York: Springer-Verlag, 2003. 151−152.

[11] Brands S, Chaum D. Distance-Bounding protocols. In: Helleseth T, ed. Proc. of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology. New York: Springer-Verlag, 1994. 344−359.

[12] Sastry N, Shankar U, Wagner D. Secure verification of location claims. In: Maughan D, Perrig A, eds. Proc. of the 2003 ACM Workshop on Wireless security (WISE). New York: ACM Press, 2003. 1−10.

[13] Meadows C, Poovendran R, Pavlovic D, Chang LW, Syverson P. Distance bounding protocols: Authentication logic analysis and collusion attacks. In: Poovendran R, *et al*., eds. Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks. Springer-Verlag, 2007.

[14] Capkun S, Hubaux JP. Secure positioning of wireless devices with application to sensor networks. In: Znati T, Knightly E, Makki K, eds. Proc. of the 24th Annual Joint Conf. of the IEEE Computer and Communications Societies. New York: IEEE Computer Society Press, 2005. 1917−1928.

[15] Zhang Y, Liu W, Fang Y, Wu D. Secure localization and authentication in ultra-wideband sensor networks. 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. In: Pascual JD, Smirnow M, eds. Proc. of the 25th IEEE Conf. on Computer Communications. Washington: IEEE Computer Society Press, 2006. 23−29.

[17] Anjum F, Pandey S, Agrawal P. Secure localization in sensor networks using transmission range variation. In: Kohno R, Prasad R, Singhal M, eds. Proc. of the 2nd IEEE Int'l Conf. on Mobile Ad-Hoc and Sensor Systems. Washington: IEEE Computer Society Press, 2005.

[18] Lazos L, Poovendran R. SeRLoc: Secure range-independent localization for wireless sensor networks. In: Jakobsson M, Perrig A, eds. Proc. of the 2004 ACM Workshop on Wireless Security. New York: ACM Press, 2004. 21−30.

[19] Lazos L, Poovendran R, Capkun S. ROPE: Robust position estimation in wireless sensor networks. In: Zhao F, Cozzens J, Estrin D, eds. Proc. of the Int'l Symp. on Information Processing in Sensor Networks. Washington: IEEE Computer Society Press, 2005. 324−331.

[20] Lazos L, Poovendran R. HiRLoc: High-Resolution robust localization for wireless sensor networks. IEEE Journal on Selected Areas in Communications, 2006,24(2):233−246.

[21] Ekici E, Vural S, McNair J, Al-Abri D. Secure probabilistic location verification in randomly deployed wireless sensor networks. Ad Hoc Networks, 2008,6(2):195−209. http://portal.acm.org/citation.cfm?id=1314716.1314987&coll=&dl=

[22] Du WL, Fang L, Ning P. LAD: Localization anomaly detection for wireless sensor networks. The Journal of Parallel and Distributed Computing, 2006,66(7):874−886.

[23] Liu DG, Ning P, Du WL. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In: Lai TH, Arora A, eds. Proc. of the 25th Int'l Conf. on Distributed Computing Systems (ICDCS). Washington: IEEE Computer Society Press, 2005. 609−691.

© 中国科学院软件研究所 http://www.jos.org.cn

[24] Li Z, Trappe W, Zhang Y, Nath B. Robust statistical methods for securing wireless localization in sensor networks. In: Zhao F, Cozzens J, Estrin D, eds. Proc. of the Int'l Symp. on Information Processing in Sensor Networks. Washington: IEEE Computer Society Press, 2005. 91–98.

[25] Liu DG, Ning P, Du WL. Attack-Resistant location estimation in sensor networks. In: Zhao F, Cozzens J, Estrin D, eds. Proc. of the Int'l Conf. on Information Processing in Sensor Networks. Washington: IEEE Computer Society Press, 2005. 99–106.

[26] Ganu S, Krishnakumar AS, Krishnan P. Infrastructure-Based location estimation in WLAN networks. In: Roberto J, Weinstein S, eds. Proc. of the IEEE Wireless Communications and Networking Conf. Los Alamitos: IEEE Computer Society Press, 2004. 465–470.

[27] Raya M, Hubaux JP. The security of vehicular ad hoc networks. In: Atluri V, Ning P, Du WL, eds. Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2005. 11–21.

附中文参考文献:

[1] 任丰原,黄海宁,林闯.无线传感器网络.软件学报,2003,14(7):1282–1290. http://www.jos.org.cn/1000-9825/14/1282.htm

[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. http://www.jos.org.cn/1000-9825/16/857.htm

曹晓梅(1974－),女,江苏无锡人,博士,讲师,主要研究领域为无线网络安全.

陈贵海(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为并行与分布式计算.

俞波(1978－),男,博士生,主要研究领域为无线传感器网络.

任丰原(1970－),男,博士,副教授,主要研究领域为网络流量管理与控制,传感器网络,系统性能评价.

© 中国科学院软件研究所 http://www.jos.org.cn