◎网络、通信、安全◎

无线传感网络安全定位和位置检测

朱 彬,廖俊国
ZHU Bin,LIAO Jun-guo

湖南科技大学 计算机科学与工程学院,湖南 湘潭 411201
School of Computer Science and Engineering,Hunan University of Science & Technology,Xiangtan,Hunan 411201,China
E-mail:binzhuhnust@gmail.com

ZHU Bin,LIAO Jun-guo.Secure locating and location verifying in wireless sensor network.Computer Engineering and Applications,2008,44(21):57-63.

Abstract: The basic function of wireless sensor network is to detect and report the position where the event happen,so location information and locating process are very important.Energy and accurate are more cared and security is ignored in location approaches in the past.Recently,the security in location is followed with interest.In this paper,the possible threaten in location and the securities in traditional location algorithm are analyzed,the exited secure location algorithm and location Verify are introduced,and the future works are proposed.

Key words: Wireless Sensor Network;location;location verifying;security

摘 要: 无线传感网络的基本功能是检测和报告事件发生的位置,所以位置发现很重要。在以前的定位协议设计过程中,只注重能耗和精度问题而忽略安全,近来定位过程中的安全问题引起了关注。分析了定位过程中可能存在的威胁,对传统的定位算法进行了安全分析,介绍了已有的安全定位算法和检测方法,并对将来的研究提出了初步的设想。

关键词: 无线传感网络;定位;安全
DOI: 10.3778/j.issn.1002-8331.2008.21.016 **文章编号:** 1002-8331(2008)21-0057-07 **文献标识码:** A **中图分类号:** TP309

1 引言

无线传感网络(Wireless Sensor Network ,WSN)的应用越来越广泛,包括军用和民用,其中有目标跟踪、环境监测、野外火灾检测等。WSN的主要作用是监测及报告有意义的事件,前提是事件发生的位置是准确的。对于基于位置的WSN应用而言,在面对恶意攻击的前提下,确保节点能检测自己的正确位置是必须的。这是因为:第一、位置信息可以判断感兴趣事件的位置,如火灾的位置、敌人战车的位置等,第二、位置可以方便许多应用服务,如目标跟踪、可以方便定位和搜救灾难中的幸存者等。第三、位置可以方便许多系统功能,如基于位置的路由[2,4,8,10,11]、基于位置的信息查询等。然而位置信息或位置发现过程受到攻击,则这些应用是不安全的,所以进行安全的定位设计是必须的。

由于节点的成本受限制,不可能每一个节点都装配全球定位系统(GPS[1]),所以位置发现协议的开发具有挑战性。在一些定位协议中,某些特殊节点或装配GPS,或已预配置了位置,这些特殊节点称为信标(Beacon)节点或锚(anchor)节点,其他节点的位置必须依靠信标信号来计算自己的位置,如果信标信号是由恶意节点提供的,其中的位置信息是错误的,或者信标节点受到攻击,那么这些协议则变得不安全。

定位像其他技术一样有安全需求。这是因为:第一、用于位置发现的信息必须可靠,所以这些信息必须可以认证。第二、用于位置发现的信息不能被篡改,所以这些信息必须是完整的。第三、所有用于计算位置的信息必须是可用的。第四、位置信息的提供者和接收者都不能否认信息交换。安全的定位技术可以分为两种:第一、安全的位置发现(secure location),这个过程是指通过安全的定位发现技术来获取位置;第二、安全的位置检测(location verify),这个过程是指所有节点通过某些定位(安全的或不安全的)技术已获得自己的位置,然后用位置检测过程计算这个位置是否正确。

目前已经开发的一些位置发现协议所关注的重点是能耗和精度,本文分析定位过程中可能的威胁,对传统的定位算法进行了安全分析,介绍了已有的安全定位算法和检测方法,并对将来的研究提出了初步的设想。

2 攻击模型

攻击可以分为内部攻击和外部攻击。内部攻击中攻击者拥有合法的身分,通过密码认证等技术这种攻击不是十分有效。外部攻击者可以妥协节点从而威胁网络。所以一个安全的位置

基金项目: 湖南省自然科学基金(the Natural Science Foundation of Hunan Province of China under Grant No.07JJ6104)。
作者简介: 朱彬(1977-),讲师,研究方向为信息安全、无线网络;廖俊国(1972-),博士,副教授,硕士生导师,研究方向为信息安全。
收稿日期: 2008-03-03 **修回日期:** 2008-05-26

发现过程必须有效地防止这两种类型的攻击。现有文献中有关攻击位置发现的类型如下。

2.1 重放(Replay)攻击

重放攻击是一种简单的攻击方式,攻击者并不需要强大的能力。此攻击主要是拥塞发送者与接收者之间的信号传输,然后重播相同的或者旧的信息。如果攻击者具有移动的能力则网络中接收到的信息是旧的几率会比较大。如果在位置发现过程中,要定位的节点受到重放攻击,接收不正确的位置参考信息,会使自己的位置计算不正确。如在图 1(a)中,攻击节点 S 把节点 A 的信息重放给了节点 B。

2.2 Sybil 攻击

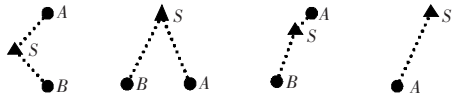
J.Douceur 在[9]文中给出了 Sybil 的概念和危害。文献[15]中分析了 WSN 中的 Sybil 攻击及防御方法。Sybil 攻击中攻击者一般声称自己有多个身分。如果在位置发现过程中,要定位的节点从同一个节点接收多个位置参考信息,则导致自己的位置不正确。如在图 1(b)中,攻击节点 S 声称有两个位置 A 和B。

2.3 蛀洞(Wormhole)攻击

Yih-Chun Hu 在[22]文中分析了 WSN 中的蛀洞攻击,[14]文中采用包控制(Packet Leashes)来防止蛀洞攻击。蛀洞攻击是所有攻击中最复杂的。一般实施者都有大的能源,有大的传输功率和范围。蛀洞攻击的实质是使两个距离很远的节点认为他们是相邻节点。如果位置发现过程与跳数等有关,则受到蛀洞攻击的几率比较大。如在图 1(c)中,攻击节点 S 使节点 A 和节点 B 相信两个节点之间只有一跳的距离。

2.4 妥协(compromise)节点攻击

如果网络中的节点被妥协,则攻击者可以使用它来传播错误的位置信息。严重的是如果信标节点被妥协,则可能整个网络的位置信息都会受到影响。如在图 1(d)中,妥协节点 S 给出的位置在节点 A。



(a)重放攻击 (b)Sybil 攻击 (c)蛀洞攻击 (d)妥协节点攻击

▲ 攻击节点 ● 节点

图 1 攻击模型

3 传统定位发现方法及安全问题

根据定位发现机制,可将现有 WSN 自身定位方法分为两类:距离相关(Range-based)和距离无关(Range-free)。即基于测距技术的定位算法和无需测距的定位算法。前者先通过测量节点间点到点的距离或角度信息(如:TOA、TDOA、AOA 等),然后使用三边测量法、三角测量法或最大似然估计法计算节点位置;后者则无需距离和角度信息,仅根据网络连通性等信息实现。距离无关定位机制在成本、功耗等方面具有优势,因此倍受关注。质心、凸规划[5,7]、DV-HOP、Amorphous、APIT 是现有的几种距离无关定位算法,它们所研究的网络模型都是由锚节点和未知节点组成的异构网络,无需任何基础设施。但这些算法在设计之初没有考虑安全因素。

3.1 质心定位算法

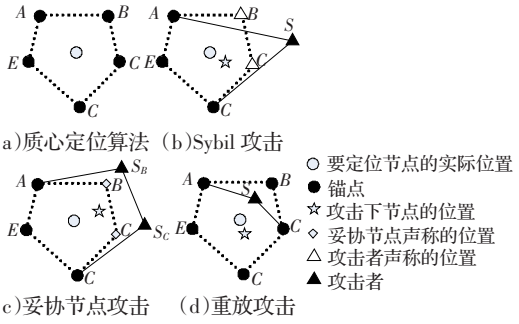
质心定位算法是南加州大学的 N.Bulusu 提出的基于网络连通性的室外定位算法[3]。质心定位算法的思想是锚节点每隔一段时间,向邻居节点广播一个信标信号,信号中包含自身 ID 和位置信息。当未知节点接收到来自不同锚节点的信标信号数量超过某一个预设门限或接收一定时间后,该节点就确定自身位置为这些锚节点所组成的多边形的质心。

正常情况:在图 2(a)中,假设要求的位置为(x,y),(X_i,Y_i)为节点 i 的位置,则 $x=(XA+XB+XC+XD+XE)/5$;$y=(YA+YB+YC+YD+YE)/5$ 为图 2(a)中要求的位置。

Sybil 攻击:在图 2(b)中,攻击节点 S 声称有两个位置 B 和 C,节点实际位置为 $x=(XA+XS+XD+XE)/4$;$y=(YA+YS+YD+YE)/4$。

妥协节点攻击:在图 2(c)中,节点 SB 和 SC 妥协,发布错误的位置 B 和 C,节点实际位置为 $x=(XA+XSB+XSC+XD+XE)/5$;$y=(YA+YSB+YSC+YD+YE)/5$。

重放攻击:在图 2(d)中,攻击节点 S 重放了 B 的位置信息。节点实际位置为 $x=(XA+XS+XC+XD+XE)/5$;$y=(YA+YS+YC+YD+YE)/5$。



(a)质心定位算法 (b)Sybil 攻击 (c)妥协节点攻击 (d)重放攻击

图 2 质心定位算法及其安全问题

3.2 DV-Hop 定位算法和 Amorphous 算法

Drago Niculescu 等利用距离矢量路由和 GPS 定位的思想提出了一系列分布式定位算法—合称为 APS,DV-Hop 定位算法是其中之一。DV-Hop 算法由三个阶段组成。首先计算未知位置节点与锚节点的最小跳数,如图 3(a)锚节点向相邻节点广播信标信息,其中包括跳数信息,初始值为 0,节点忽略来自相同锚节点的较大跳数,将跳数加 1 后转发。第二阶段,在获得其它锚节点位置和相隔跳数后,锚节点计算网络平均每跳距离,然后将其作为一个校正值广播至网络中。校正值采用可控洪泛法在网络中传播,这意味着一个节点仅接受获得的第一个校正值,而丢弃所有后来者,这个策略确保了绝大多数节点从最近的锚节点接收校正值。当接收到校正值后,节点根据跳数计算与锚节点距离。其公式为:

$$HOPsize_i=\frac{\sum_{j\neq i}\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{\sum_{j\neq i}h_j}$$

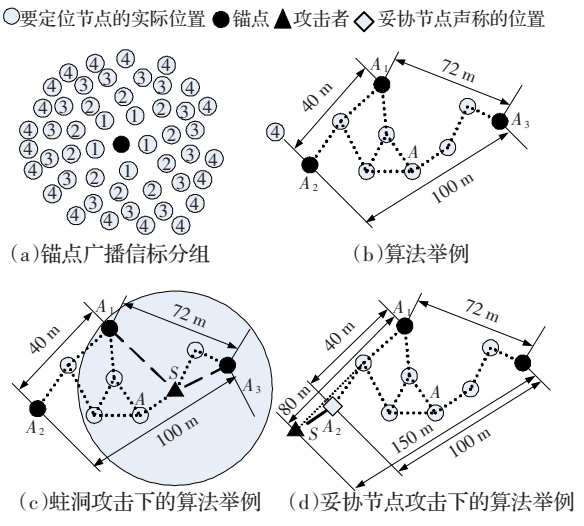
(x_i,y_i)、(x_j,y_j)为节点 i、j 的位置,h 为 i 与 $j(i\neq j)$之间的跳数。当未知节点获得与三个或更多锚节点的距离,则在第三阶段执行三边测量或极大似然法计算自己的位置。

正常情况:在图 3(b)中,锚节点 $A1$ 和锚节点 $A2$ 之间的跳数为 2,锚节点 $A2$ 和锚节点 $A3$ 之间的跳数为 5,则锚节点 $A2$ 计算网络中的每跳平均距离为(40+72)/(2+5)=16,如果节点 A 从锚节点 $A2$ 处获得平均每跳距离,则它与三个锚节点之间的距离分别为 $A1$:3×16=48,$A2$:2×16=32,$A3$:3×16=48。

蛀洞攻击:在图 3(c)中,攻击节点 S 在锚节点 $A1$ 和锚节

点 $A2$ 建立了蛀洞链接,使得锚节点 $A3$ 和锚节点 $A2$ 之间的跳数为 2,则锚节点 $A2$ 计算网络中的每跳平均距离为(40+72)/(2+2)=28,如果节点 A 从锚节点 $A2$ 处获得平均每跳距离,则它与三个锚节点之间的距离分别为 $A1$:3×28=84,$A2$:2×28=54,$A3$:2×28=54。

妥协节点攻击:在图 3(d)中,攻击节点 S 是被妥协节点,它声称自己的位置是在 $A1$。实际上,锚节点 $A2$ 计算网络中的每跳平均距离应该为(80+72)/(2+5)=21.74,如果节点 A 从锚节点 $A2$ 处获得平均每跳距离,则它与三个锚节点之间的距离分别为 $A1$:3×21.74=65.22,A2:2×21.74=43.48,A3:3×21.74=65.22。



(a)锚点广播信标分组　(b)算法举例　(c)蛀洞攻击下的算法举例　(d)妥协节点攻击下的算法举例

图 3　DV-HOP 定位算法及其安全问题

Amorphous 算法[26]与 DV-HOP 算法所面临的安全问题相同。

3.3　APIT 算法

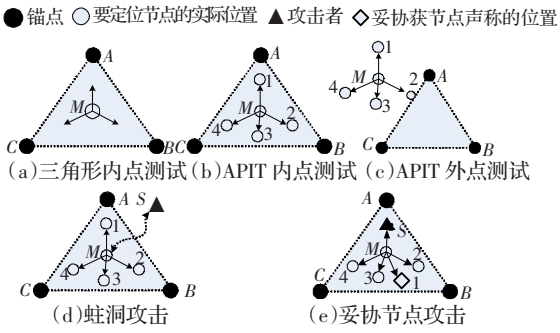
T.He 等在[12]文中提出了近似三角形内点测试法 APIT。APIT 算法的理论基础是:假如存在一个方向,沿着这个方向 M 点会同时远离或接近 A、B、C,那么 M 位于 ΔABC 外;否则,M 位于 ΔABC 内,如图 4(a)。为了在静态网络中执行内点测试,定义了近似内点测试(APIT):假如节点 M 的邻居节点没有同时远离或靠近三个锚节点 A、B、C,那么 M 就在 ΔABC 内;否则,M 在 ΔABC 外。它利用 WSN 较高的节点密度来模拟节点移动和在给定方向上,一个节点距锚节点越远,接收信号强度越弱的无线传播特性来判断与锚节点的远近。通过邻居节点间信息交换,仿效三角形内点测试的节点移动,如图 4(b),节点 M 通过与邻居节点 1 交换信息,得知自身如果运动至节点 1,将远离锚节点 B 和 C,但会接近锚节点 A,与邻居节点 2、3、4 的通信和判断过程类似,最终确定自身位于 ΔABC 中;而在图 4(c)中,节点 M 可知假如自身运动至邻居节点 4 处,将同时远离锚节点 A、B、C,故判断自身不在 ΔABC 中。

蛀洞攻击:在图 4(d)中,攻击节点 S 与 M 之间建立了蛀洞链接,通过信息交换,M 可知假如自身运动至 S 处,将同时远离锚节点 A、B、C,故判断自身不在 ΔABC 中。

妥协节点攻击:在图 4(e)中,攻击节点 S 是被俘节点,它声称自己的位置在 1,同时更改与锚节点 A 的接收信号强度。使得 M 无法完成近似内点测试。此攻击的第二个威胁是增加了位置的误差。

3.4　对与距离有关的定位方法的攻击

S.Capkun 在文[24]中提出了对于已有的一些距离有关的定位系统的攻击。



(a)三角形内点测试 (b)APIT 内点测试 (c)APIT 外点测试　(d)蛀洞攻击　(e)妥协节点攻击

图 4　APIT 定位算法及其安全问题

3.4.1　对 GPS 定位系统的攻击

GPS 定位系统不适合室内定位。而民用 GPS 更不能用于安全定位,因为民用 GPS 很容易被 GPS 卫星模拟器所欺骗,这种模拟器能发射比正常卫星信号更强的信号,而很多欺骗性攻击是很难检测的。军用 GPS 通过编码能够解决这个问题。假设一个移动节点通过 GPS 取得正确的位置,控制者或其他移动节点没有办法校验这个位置的正确性,除非它们装配有可信校验的软件或硬件模块。

3.4.2　对于超声波定位系统的攻击

超声波定位系统的操作是通过在两个节点之间测量声音信号的飞行时间(ToF,Time of Flight)。如果在系统中使用 RF信号,则发送者和接收者之间不需要时间同步。由于室外存在干扰,所以超声波定位系统只适于室内。超声波定位系统很容易通过内部攻击或外部攻击减少或增加距离。为了减少两个真实节点之间距离,两个攻击者使用 RF 信号并以快超声波几倍的速度发送信号,而通过拥塞(jamming)和在稍后延迟的时间内重放(replay)信号则可扩大距离。内部攻击都通过修改信号发送或接收的次数或者简单地延迟自己对于信号的反应增加或减少距离。

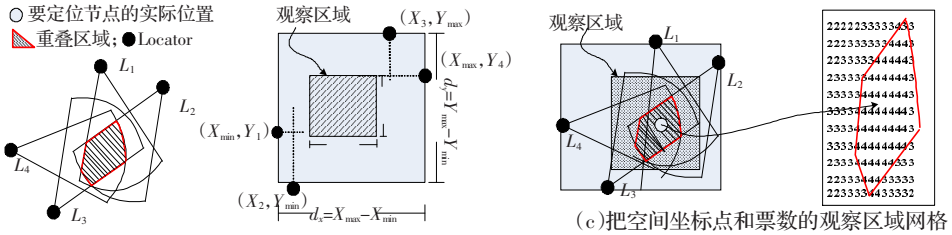
3.4.3　对于射频定位(RF)系统的攻击

RF 系统依赖于检测接收信号强度(Received Signal Strength,RSS),内部攻击者只要报告一个错误的能量级别就可以攻击到一个可信节点距离。位于两个可信节点之间的外部攻击者则可以通过拥塞(jamming)它们之间相互通信,然后以更高或更低的能量级别重放(replay)信号来攻击测距。

4　安全的定位技术和校验方法

4.1　SeRLoc

Lazos 和 Poovendran 首次提出了在 WSN 中进行安全定位的方法 SeRLoc。SeRLoc 是分布式的、与距离无关的、资源高效率的定位技术,在位置发现的过程中未知位置节点之间不需要额外的通信。对于蛀洞攻击、Sybil 攻击、节点妥协攻击,SeRLoc 具有鲁棒性。SeRLoc 由两种节点构成:一种装配了全向(omnidirectional)天线的普通节点和另一种装配了 directional 天线的定位器(Locator)。节点通过接收 Locator 的信标来进行定位。每一个 Locator 在每一个天线扇区上传送不同的信标,信标包括两个信息:Locator 的位置和以一个全局轴线为准的天线的边界线的角度。SeRLoc 的位置过程如图 5 所示:第一步,节点收集它所能听到的 Locator 的信息;第二步,节点计算一个可以定位自己的观察区域;第三步,节点决定所有扇区的重叠区域,



(a)节点侦听 L_1~L_4,估计在扇区重叠区域的重心　(b)决定观察区域　(c)把空间坐标点和票数的观察区域网格和扇区重叠区域放在一起,节点用票数最高的区域的重心为自己的坐标

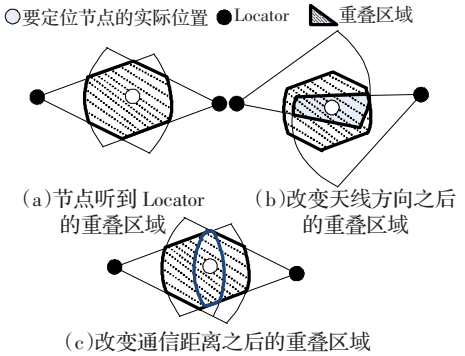
图 5　SeRLoc 发现位置过程

并采用网格分数系统用票数来定义重叠区域;第四步,用最高票数的网格的质心估计自己的位置。SeRLoc 用 RC5 加密所有的信标信号，并用有效的单向哈希函数认证Locator 的 ID。在 SeRLoc 中,攻击者只有俘虏几个 Locator 才能攻击位置发现过程。节点计算自己的位置不依赖其他节点,Sybil 攻击不会有效。因为有唯一扇区和不能违反通信距离的两个特征，所以 SeRLoc 可以防止蛀洞攻击。在 SeRLoc 中,为了提高定位精度,必须使用更多的 Locator 或 directional 天线。作者假设没有无线干扰,与真实环境不相符。

4.2　HiRLoc

Lazos 和 Poovendran 在文[21]中提出了另外一种与距离无关的安全定位算法 HiRLoc。在 HiRLoc 中,节点消极地检测自己的位置,节点之间不需要相应的通信。HiRLoc 不需要额外的硬件,对于 Locator 密度的需要减少了。根据天线方向和通信距离的变动来抵抗蛀洞攻击、Sybil 攻击、节点妥协攻击。

HiRLoc 发现位置过程如图 6,节点接收 Locator 的信标,信标包括 Locator 的位置、以一个全局轴线为准的天线的边界线的角度和 Locator 的通信范围。HiRLoc 有两种计算重叠区域的方法,第一种是计算所有扇区的重叠区域:第一步,初始化估计扇区重叠区域,其大小由所听到 Locator 的坐标决定;第二步,收集信标,Locator 发布多个信标,包括:改变天线方向、改变通信距离以及混合操作。这种操作可以减少重叠区域从而提高精度。第三步,决定重叠区域;第二种是计算每一个传输段的重叠区域。决定重叠区域后,再采用与 SeRLoc 中相同的方法,用网格分数系统中最高票数的区域的质心来估计自己的坐标。HiRLoc 用全局共享密钥加密信标传输，并用防冲撞哈希函数对信标传输认证。HiRLoc 不需要测量距离,可以防止改变测量的攻击,另外节点发现位置不需要其他节点协同,所以可以抵抗节点妥协攻击。



(a)节点听到 Locator 的重叠区域　(b)改变天线方向之后的重叠区域

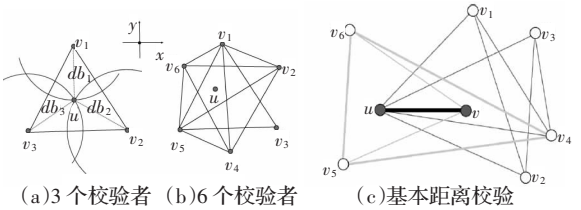
(c)改变通信距离之后的重叠区域

图 6　HiRLoc 发现位置过程

4.3　SPINE

S.Capkun 和 J.-P.Hubaux 提出一种技术 Verifiable Multilateration(VM):通过一系列的已知位置节点的参考来计算一个节点的位置，用可认证的距离范围来保证节点的精确定位。基于 VM,作者提出了 WSN 中安全定位的方法 SPINE。SPINE 通过限制每一个节点和至少三个位置参考点之间的距离来定位。基于攻击者或要求位置发现者不能缩减与参考点之间的距离而只能扩大这一特征,VM 可以进行距离限制。由于有纳秒级精确的时间，节点在范围内能限制与任何一个参考点的距离。假设任何攻击者不能与被俘的节点勾结,如果一个节点在由三个参考点所组成的三角形中,通过 VM 提供的健壮的位置估计,则节点可以计算自己的位置。VM 可以有效防止蛀洞攻击、欺骗攻击、拥塞攻击,阻止不诚实节点谎报自己的位置。如果要执行 VM,则网络必须布置很多的参考点。

VM 的过程如图 7(a):第一步 u 点传输范围内的 3 个节点 V_1、V_2、V_3 测试与 u 的距离 db_1、db_2、db_3;第二步计算 u 的估计位置;第三步,根据所计算的估计位置进行两个测试:距离测试和内点测试。如果两个测试都通过则接受估计位置,否则抛弃。在计算估计位置时用集中式的方式,增加基站的压力。SPINE 算法的过程要为三步:第一步,节点测量与相邻节点之间的距离界限;第二步,用 VM 校验距离界限;第三步,节点采用分布式或集中式算法计算节点的位置。其中 BDV 的校验过程如图 7(c):第一 u 和相邻节点构造包围 v 的三角形,第二 v 和相邻节点构造包围 u 的三角形,第三构造包围 u 和 v 的三角形。图中 u 和相邻节点构造包围 v 的三角形有 $\Delta(u,V_1,V_2)$、$\Delta(u,V_1,V_4)$、$\Delta(u,V_2,V_3)$、$\Delta(u,V_3,V_4)$,而构造包围 u 和 v 的三角形只有 $\Delta(V_5,V_4,V_6)$,所测得的距离 db_{uv}(从 u 至 v)和 db_{vu}(从 v 至 u)用 VM 方法在所有构造的三角形中校验。这样构造三角形的节点可以定义一个本地坐标系统来算计 u 和 v 的位置。



(a)3 个校验者　(b)6 个校验者　(c)基本距离校验

图 7　VM 校验

4.4　ROPE

Lazos,Poovendran 和 Capkun 在文[20]中提出了一种健壮的定位算法 ROPE。ROPE 把节点分为 Locator 和 Sensor,允许 Locator 在网络中广播位置信息使 Sensor 可以检测自己的位置,校验传感信息源,并把 Locator 作为数据收集点。ROPE 可以提供位置决定和位置校验。ROPE 有两个优点:一是允许所有节点不需要集中计算而决定自己的位置,二是通过节点声称

的位置可以先于数据收集而被校验的长处提供位置校验功能。每一个 Locator 和每一个 Sensor 共享一个对密钥。Locator 的数量少，不需要增加 Sensor 太多的存储空间。

图 8(a)中 s 定义了它所能听到的 Locator 集合 $LHs=\{L1\sim L4\}$，可以执行测量距离界限的 Locator 集合 $LDBs=\{L3,L4\}$，$|LDBs|<3$，s 不能被一个三角形包围。s 还定义一个距离界限交叉区域 DBIR。由于在 DBIR 中如果 s 扩大它与 $L3$，$L4$ 的距离界限，则它可以任意定位，所以可以用 Sensor-Locator 的通信范围作限制。图 8(b)s 定义了它所能听到的 Locator 集合 $LHs=\{L1\sim L4\}$，可以执行测量距离界限的 Locator 集合 $LDBs=\{L1\sim L4\}$，s 还定义一个距离界限交叉区域 DBIR，并在 DBIR 中计算扇区重叠区域 ROI。图 8(c)给出了位置校验过程，因为 Locator 作为数据收集点，只有它可以接收数据报告，所以 $L3$ 可以校验 s 声称与它的距离界限，这个界限可以扩大，但这样对于攻击者来说是没有用的，因为一个 Sensor 不可能用超自己通信范围来与 Locator 报告数据。

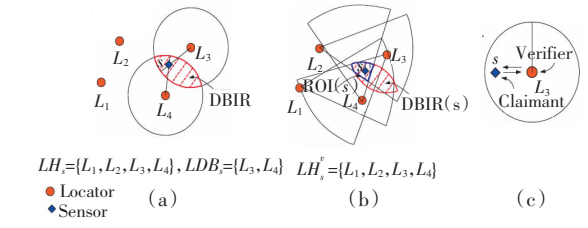


图 8　ROPE 的位置发现和校验过程

ROPE 提出了一种新的度量原则叫 Maximum Spoofing Impact 用来度量 ROPE 中的攻击。只须有少量的参考点，ROPE 就可以达到很低的 Maximum Spoofing Impact。ROPE 可以抵抗拥塞攻击、蛀洞攻击和节点被俘攻击。

ROPE 只适合小型网络，在定位过程中要执行加密、XOR 等运算，并且要求有很严格的时钟同步。

4.5　以基础建设为中心（infrastructure-centric）和以节点为中心(node-centric)的安全定位

Srdjan C̆、Mario C̆ 和 Mani 在文[23]中提出了利用隐藏和移动基站进行安全定位的方法。目的在于抵抗两种攻击：内部攻击和外部攻击。以节点为中心的定位是指节点从基站接收位置信号用来计算自己的位置；以基础建设为中心的定位是指通过双方相互通信来计算节点的位置。

以基础建设为中心的定位采用分时到达（Time Difference of Arrival），基站是隐藏的，只能听到节点所发的信标。图 9 说明了定位的过程，节点 A 发送信标，基站 CBS1~CBS4 测量信号到达自己的时间 $t1\sim t4$，然后计算 A 的位置，校验是否与不同时间一致。这种方法基于攻击猜测节点位置的几率很小，可以同时抵抗内外攻击。在以节点为中心的定位中假设节点已经通过非安全的方法取得，然后提供一个安全的信赖于隐藏基站的位置校验协议。在图 10 中，节点 A 把自己的位置 PF 报给 CBS，CBS 测得它与 A 的距离 d_F^m，然后根据所测距离来校验PF。

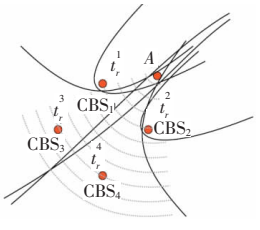


图 9　分时到达定位

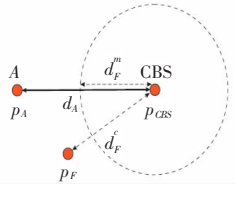


图 10　位置校验过程(利用隐藏基站)

在利用移动基站(Mobile Base Station，MBS)进行位置校验的过程中，如图 11，当 MBS 在时间 $t1$ 和位置 PMBS($t1$)发送一个信息包括一个质问(challenge) nounce 和时延 TR，这个信息相邻节点必须回复。在时间 TR 内，MBS 移动到位置 PMBS($t2$)，这个位置是 PMBS($t1$)所定义的通信范围之内。在位置 PMBS($t2$)MBS 收到节点的回复后，计算距离并校验位置。

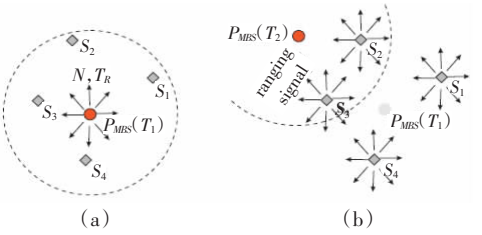


图 11　位置校验过程(利用移动基站)

4.6　反攻击位置估计(Attack Resistant Location Estimation)

Liu，Ning 和 Du 在文[18]中提出了两种健壮的基于距离的方法来容忍在基于信标的位置发现协议中的恶意攻击。第一种方法反攻击最小均方差估计，这种方法以最小均方差估计作为指标，通过检查不同信标信号中的位置参考信息的不一致来过滤恶意的信标信号。第二种方法是基于票数的位置估计，这个方法把撒播区域量化成一个网格，每一个网格单元上都有一个位置参考票数。通过采用正确的票数方法来容忍攻击。如果攻击者能够妥协一个简单的主要的距离估计，这种方法就会失效。如果攻击者有 κ 个相邻节点，那么只要妥协$\lfloor\frac{\kappa}{2}\rfloor+1$ 个信标节点，就能够产生比开始更多的恶意的位置参考。这样使得相邻节点的最小均方差估计错误，然后这个错误会在整个网络中传播。

4.7　信标套件(Beacon Suite)

Liu、Ning 和 Du 在文[19]中为紧急事情应用中的定位设备提供了一套可以检测给出不正确的位置参考的信标节点的技术，包括：检测恶意信标节点、检测重放信标信号、鉴别恶意信标节点、避免错误检测、取消恶意信标节点等。这种技术中的信标节点有两种作用：提供位置信息和检测它所听到的其他信标节点。信标节点可以请求进行位置停息。他们把信标分为检测节点((detecting node)用于检测)和目标节点((target node)被检测)。在每一个信标节点上有两个计数器：警报次数(alert counter)和报告次数(report counter)，警报次数记录该节点被相应信标节点报告的可疑次数，报告次数记录节点报告可疑节点的次数。如果检测节点检测出节点行为异常则报告给基站。当所疑目标节点没有被取消且检测节点的报告次数低于一个阈值时，警报次数增加。

4.8　DRBTS

Srinivasan、Teitelbaum 和 Wu 在文[27]中提出了一种分布式基于信任和委托的安全协议来提供安全定位的方法。在这种方法中，恶意信标节点提供的错误信息可以被拒绝。DRBTS 是第一个用信任度来排除恶意信标节点的模型。在 DRBTS 中，每一个信标节点(BN)监视 1 跳的相邻节点，侦测信标节点是否有不当行为，如果则更新相应的邻居信任度表(Neighbor-Rep-

表1 安全定位技术比较

名称	采用安全方法	存储开销/(byte/节点)	能量开销(通信量或计算量)	误差	信标节点数	计算方式
SeRLoc	(1)加密(RC5) (2)认证(高效单向哈希函数)	$L\times8$(L 为信标结点数)	要传输$\lfloor mL\rfloor$个信标(m 是扇区数,L 是信标结点数)	低	少	分布式
HiRLoc	(1)全局共享密钥加密信标传输。使用伪随机函数减少存储开销 (2)用防冲撞哈希函数对信标传输认证	预配置包含信标的 ID 和相应的哈希值	与要求的定位精度有关	低	少	分布式
SPINE	(1)校验者和申请者共享密钥 (2)消息认证码(MAC) (3)加密	小	要进行加密、XOR 运算、快速信息交换	依赖于网络的连通性	依赖于精度	分布式或集中式
ROPE	(1)共享对钥加密,使用伪随机函数减少存储开销 (2)认证(单向哈希函数)	存储对密钥	1 个信标/扇区	低	少	分布式

表2 安全位置校验

名称	存储开销	误差	信标节点数	测距方式
Attack Resistant MMSE	依赖于参考点的多少	参考点多于一定数时比 Voting 低	依赖于估计精度	简单 RSSI
Location Estimation Voting	依赖于参考点的多少	参考点少于一定数时比 MMSE 低	依赖于估计精度	
Beacon Suite	密钥建立和加密操作	依赖于诊断 ID 数和诊断率	节点数×10%	由信标的收发估计

utation-Table,NRT),基于一个法定票数方法,节点可以选择哪一个可以信任。如果节点要用一个 BN 的信息,它必须从他们共同的相邻节点取得至少一半以上的信任票数。节点使用一个简单的投票方法来估计它的范围内的 BN 的信任度。在此模型中,节点可以得到任何它已知 BN 的行为状态,可以得到系统的破坏等级。分布式模型可以减轻基站的压力,减少因意信标节点提供不正确信息而造成的破坏。

5 分析与比较

在传统的与距离无关定位中,因为依赖于数据包交换来测距,所以数据包的安全性应该是此类算法中在安全方面关注的重点,密码学上的技术可以解决一些问题,但因此也增加了网络的通信开销,还有一些问题是密码学方法无法解决的,则只能依赖增加硬件或修改协议,这会使得成本增加,而且也使得能量消耗更大。而在与距离相关的技术中,上面所述对于这类技术的攻击可以看作是对硬件的攻击,而此种攻击最难于检测,这对与之相关的定位系统来说应该是致命的。对于以上几种安全的定位技术和位置检测技术,没有一个统一的衡量标准。从无线传感网的特点出发,用所用安全方法、存储开销、位置误差、锚节点数、能量开销等参数进行分析和比较,表 1 分析了主要的安全定位技术,表 2 则比较了两种主要的位置检测技术。

6 将来的工作和研究方向

在 WSN 中,定位技术除了对精确度和能耗的研究之外,安全也是研究方向之一。节点的安全定位包括两个方;的内容,一是节点如何安全地确认或者计算自己的位置信息;另一方面是节点如何安全地确认其他节点的位置信息。定位方法与网络的应用及使用环境密切相关,其所需安全等级也不相同,在将来的设计中定位方法的安全应该把这些因素也考虑到进去,并设计与之相应的安全措施。下面是几个可以的研究方向:

(1)在与距离无关的相关算法中,用跳数等来估计距离,和路由算法一样,这些限制条件成为了攻击的对象,如何对之进行有效的保护,这些与加密及密钥管理有密切的关系,需要进一步研究。

(2)在与距离相关的相关算法中,用来测量距离的技术可能被攻击者利用,使得所测距离不准,如何对这些技术加强其安全性应该是挑战之一。

(3)研究方向的另一个是位置校验技术,对已经取得的位置进行有效的校验是必须的,目前这个方向已经展开,但现有的技术计算比较复杂。如果进行简单而有效的校验是下一步的研究方向。

(4)在以位置为基础的路由算法中,位置发现及路由过程中位置成为主要的攻击对象,如何对其进行有效的安全设计是可能的研究方向。

7 总结与展望

无线传感网的应用越来越广泛,其中很多应用都跟位置有关系。以前的定位协议设计都集中考虑能耗和精度,而很少考虑安全。在对于已有的安全技术进行分析后,我们认为安全的定位技术的将来的设计应该符合下面几个方面:(1)低能耗;(2)高精度;(3)具有安全性;(4)应该是分布式的;(5)从成本节约的方面来说,应该不依赖于基础设施,应该是与距离无关的。我们认为位置检测和安全定位一样重要,因为即使开始位置是正确,在某些应用中,还必须判断位置的正确性。在设计的过程,应该和其他协议混合设计,如:密钥管理等,在能耗方面,应该进行跨层设计等。

本文对定位过程作了一个综合叙述,讨论了在定位中面对的安全问题,讨论了传统技术中会出现的安全问题,并对已有的安全定位方法和位置估计作了初步的探讨,希望可以给研究者和兴趣者有帮助。

参考文献:

[1] Wellenhoff B H,Lichtenegger H,Collins J.Global positions system: theory and practice[M].4th ed.[S.l.]:Springer Verlag,1997.

[2] Ko Y B,Vaidya N H.Location-aided routing(lar) in mobile ad hoc networks[C]//proceedings ACM/IEEE MOBICOM 98,October 1998:66-75.
[3] Bulusu N,Heidemann J,Estrin D.GPS-less low cost outdoor localization for very small devices[J].IEEE Personal Communications Magazine,2000,7(5):28-34.
[4] Karp B,Kung H T.GPSR:greedy perimeter stateless routing for wireless networks[C]//Proceedings of ACM MobiCom 2000,2000:243-254.
[5] Doherty L,Pister K S,Ghaoui L E.Convex optimization methods for sensor node position estimation[C]//Proceedings of IEEE.INFOCOM'2001,Anchorage,April 2001.
[6] Nicolescu D,Nath B.Ad-hoc positioning systems(APS)[C]//Proceedings of IEEE GLOBECOM 2001,San Antonio,TX,USA,November 2001.
[7] Doherty L,Pister K S J,El Ghaoui L.Convex position estimation in wireless sensor networks[C]//INFOCOM 2001.Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies.IEEE,2001,3:1655-1663.
[8] Xu Y,Heidemann J,Estrin D.Geography-informed energy conservation for ad hoc routing[C]//Proceedings of ACM MobiCom 2000,Rome,Italy,July 2001.
[9] Douceur J.The sybil attack[C]//Proc of IPTPS 2002,Cambridge,MA,USA,March 2002.
[10] Hong X,Xu K,Gerla M.Scalable routing protocols for mobile ad hoc networks[J].IEEE Network Magazine,2002(4).
[11] Rao A,Ratnasamy S,Papadimitriou C,et al.Geographic routing without location information[C]//Proceedings of ACM MOBICOM 2003,2003:96-108.
[12] He T,Huang C,Blum B,et al.Range-free localization schemes in large scale sensor network[C]//Proc of MOBICOM 2003,San Diego,CA,USA,September 2003.
[13] Nagpal R,Shrobe H,Bachrach J.Organizing a Global coordinate system from local information on an Ad hoc sensor network[C]//Proc of IPSN 2003,Palo Alto,USA,April,2003.
[14] Hu Y,Perrig A,Johnson D.Packet leashes:a defense against wormhole attacks in wireless Ad hoc networks[C]//Proceedings of INFOCOM 2003,San Francisco,CA,USA,April 2003.
[15] Newsome J,Shi E,Song D,et al.The sybil attack in sensor networks:analysis and defenses[C]//Proceedings of IPSN 2004,Berkeley,CA,April 2004.
[16] Lazos L,Poovendran R.SeRLoc:secure range independent localization for wireless sensor networks[C]//ACM Workshop on Wireless security(ACM WiSe'04),Philadelphia,PA,October 1,2004.
[17] Capkun S,Hubaux J P.Secure positioning of wireless devices with application to sensor networks[C]//Proceedings of IEEE INFOCOM'05,2005.
[18] Liu D,Ning P,Du W.Attack-resistant location estimation in sensor networks[C]//Proceedings of The Fourth International Conference on Information Processing in Sensor Networks(IPSN'05),2005:99-106.
[19] Liu D,Ning P,Du W.Detecting malicious beacon nodes for secure location discovery in wireless sensor networks[C]//25th IEEE International Conference on Distributed Computing Systems(ICDCS'05),2005:609-619.
[20] Lazos L,Poovendran R,Capkun S.ROPE:Robust position estimation in wireless sensor networks[C]//Proceedings of the 4th International Symposium on Information Processing in Sensor Networks,IPSN'05,2005.
[21] 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.
[22] Hu Yih-Chun,Perrig A,Johnson D B.Wormhole attacks in wireless networks.Selected Areas in Communications[J].IEEE Journal,2006,24(2):370-380.
[23] Capkun S,Cagalj M,Srivastava M.Securing localization with hidden and mobile base stations[C]//Proceedings of IEEE INFOCOM,2006:1-12.
[24] Capkun S,Hubaux J P.Secure positioning in wireless networks[J].IEEE Journal on Selected Areas in Communications,2006,24(2):221-232.
[25] Zhang Qing,Yu Ting,Ning Peng.A framework for identifying compromised nodes in sensor networks[C]//Proceedings of 2nd IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks(SecureComm 2006),August 2006.
[26] Nagpal R.Organizing a global coordinate system form local information on an amorphous computer.AI Memo 1666,MIT AI Laboratory,August 1999.
[27] Srinivasan A,Teitelbaum J,Wu J.DRBTS:distributed reputation-based beacon trust system[C]//2nd IEEE International Symposium on Dependable,Autonomic and Secure Computing(DASC'06),2006:277-283.
[28] 孙利民,李建中,陈渝,等.无线传感网络[M].北京:清华大学出版社,2005.

(上接56页)

雷达,较好地解决了毫米波收发前端与NI数据采集卡的匹配问题。完成了一套实用的汽车防碰撞报警系统。该系统可方便地移植到DSP单片机环境,同时,它又可作为一个汽车动态性能监测平台,通过添加传感器,可以对汽车综合性能进行实时测量。

参考文献:

[1] 吕立波.汽车避撞技术及其发展[J].国外科技动态,2002(6):20-22.
[2] 向敬成,汪学刚.3mmFMCW雷达及信号处理技术[J].火控雷达技术,1995,24(3):15-19.
[3] 刘刚,侯德藻.汽车主动避撞系统安全报警算法[J].清华大学学报:自然科学版,2004,44(5):697-700.
[4] Ayres T J,Li L,Schleuning D,et al.Preferred time-headwar of highwar drivers[C]//IEEE Intelligent Transportation Systems Conference Proceedings,Oakland(CA),USA,2001.
[5] 程震先,恽雪如.汽车防撞雷达的数据处理[J].北京理工大学学报,1995,15(2):212-217.
[6] 丁康,江利旗.离散频谱的能量重心校正法[J].振动工程学报,2001,14(3):354-358.
[7] ZHANG Da-biao,WANG Yan-ju,WANG Yu-tian,et al.Research of velocity and distance measuring system based on millimeter-wave radar[C]//ISIST'2004,2004,3:1081-1086.
[8] LabVIEW7Express Measurements Manual[J].National Instruments,2003,13:1-5.