抵抗恶意信标的安全优化 DV-Hop 算法①

黄晨钟，许 力，叶阿勇，钟进发

(福建师范大学 网络安全与密码技术重点实验室，福州 350007)

摘 要：信标节点在无线传感器网络定位算法中起着关键作用，然而信标节点的安全常常被忽视。针对恶意信标节点发送虚假位置信息这种较常见且破坏性较强的攻击方式，在 DV-Hop 定位算法的基础上提出了一种抵抗恶意信标的安全 DV-Hop 定位算法。该算法利用信标之间的距离约束来隔离恶意信标节点，同时采用多信标校正值权衡的策略克服了信标比例下降与残余恶意信标对定位结果带来的不利影响，提高定位的准确性和安全性。

关键词：无线传感器网络；DV-Hop；定位安全

Secure DV-Hop Algorithm Against Malicious Beacon Nodes

HUANG Chen-Zhong, XU Li, YE A-Yong, ZHONG Jin-Fa

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

Abstract: The beacon nodes play a key role in the process of unknown nodes' localization in wireless sensor networks' localization algorithms. However, the security of beacon nodes is often overlooked. A secure and optimal DV-Hop localization algorithm is proposed against malicious beacon nodes which send false location information in this paper. The proposed algorithm isolates malicious beacon nodes by the scheme of beacon-distance constraint and overcomes negative factor which is caused by the decline of beacon nodes' ratio and remaining malicious beacon nodes by the scheme of multi-correction balance. It improves the correction and security performance of localization algorithm.

Key words: wireless sensor networks; DV-Hop; secure node localization

1 引言

无线传感器网络通常由普通传感器节点与信标节点构成。普通传感器节点不具有自身定位功能，信标节点由人工部署事先获知位置信息或者装配 GPS 定位设备。传统的传感器网络定位的研究多集中于定位精度、节点能量、通信代价等方面，定位机制的安全性并没有引起研究人员足够的重视。基于传感器网络节开放性部署的特点，节点容易被俘获，在定位过程中，对信标节点、普通传感器节点、信标报文发起的攻击，称之为定位攻击[1]。 特别针对信标节点的攻击，是较常见的也是破坏性较大的一类定位攻击方式。本文针对恶意信标节点位置欺骗的攻击方式，在 DV-Hop 定位算法的基础上提出一种基于信标验证的安全信标的优化算法。

2 相关工作和问题描述

2.1 节点安全性分析

从安全性方面考虑，传感器网络节点可分为两类：可信节点与恶意节点。可信节点指的是安全的角度上的合法节点，不受外界控制，不窃取网络数据信息，不会对其它节点进行有目的的人为破坏。恶意节点指被敌方俘获的网络节点或有意部署的攻击节点，对网络中的其它节点有危害的非法节点。在本文中，敌方俘获网络自身节点的发起的攻击方式称之为内部攻击，敌方通过人为方式部署恶意节点发起的攻击，称之为外部攻击。

无线传感器网络信标节点在定位过程中起着关键作用，信标节点的位置信息是待测节点实现定位的必要条件。不可靠信标节点的位置（坐标）信息势必使

① 基金项目:国家自然科学基金(61072080);福建省自然科学基金(2009J01274)
收稿时间:2011-01-22;收到修改稿时间:2011-02-25

得定位的结果产生巨大的误差。本文主要针对被敌方俘获信标节点发起位置欺骗的内部攻击方式进行可信验证，并尽可能减少隔离恶意信标节点对定位服务质量造成的影响。

2.2 恶意节点检测技术

Liu 等人提出一种检测和移除被俘获的信标节点的机制[2]。其检测原理如下，检测信标节点 v 以未知节点的身份向被检测信标节点发送 u 定位请求信息 REQ。信标节点 u 响应请求信息，发送包含有自身位置信息的数据包给检测方 v。检测方 v 参考响应信息，判断被检测信标节点 u 的合法性，该恶意信标安全检测机制需要通过其它方式获取距离信息，对一些具体的定位算法未必适用。文献[3]提出了一种源点编码与多路径传送的检测方案，根据解码的结果判断路径上是否存在恶意节点，但由于需要多路径传输，节点通信与能量消耗代价较大。文献[4]提出了一种基于投票的定位估计的抵抗攻击方法，实现鲁棒性定位。Srinivasan 等人引入声誉机制建立信标节点间的声誉信息，待测节点通过信任度选出可信信标节点，减小恶意节点对定位的影响[5]。我们在前期工作中提出利用各信标的校正值均值衡量整体网络的节点密度信息，利用跳数距离验证，减小了恶意信标节点对网络单跳距离的影响[6]，本文在此基础上提出基于信标间距安全验证和多信标校正的防恶意信标节点的 DV-Hop 改进算法。

2.3 位置欺骗攻击模型

无线传感器网络节点开放性部署，大部分节点无人维护，部分信标节点易被敌方俘获成为恶意信标节点。以图 1 为例，M_1 为被敌方俘获的信标节点，其实际的位置坐标为 (x_1,y_1)，其恶意虚报的位置坐标为 (x_1',y_1')；A_2、A_3 为可信的信标节点；D_1、D_2 为 M_1 到 A_2、A_3 之间的真实距离，D_1'、D_2' 为参考虚报的位置信息计算所得上述节点间不可靠的欧式距离。本文中假定信标节点之间的跳数信息是安全可信的，恶意信标节点发布虚假的位置信息。恶意信标虚报的位置信息在定位过程中的威胁主要有两个方面：

①信标节点无法计算获得正确的节点间的距离数据。

特别在 DV-Hop 算法中，信标节点利用信标之间的距离与跳数信息计算节点之间的平均单跳校正值，根据恶意信标节点虚假的位置信息计算得到的信标间的欧式距离 D_1'、D_2' 是不可靠的，势必给待测节点的定位结果带来巨大的误差。在本文中，主要防御此类安全威胁。

②节点能量耗尽。

由于传感器节点能量受限，如果恶意信标节点发布大量虚假的位置信息，节点电池能量与信道的通信带宽将很快耗尽，使得网络瘫痪，无法正常工作。

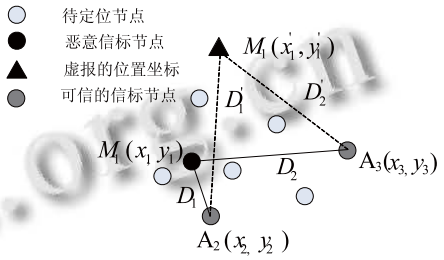

图 1　位置欺骗攻击

3　抵抗恶意信标的安全优化DV-Hop算法

3.1 信标间距约束的安全验证

针对恶意信标节点位置欺骗攻击通过虚报位置信息影响待测节点的定位结果，提出了新的防恶意信标的安全定位算法，其中基于信标间距约束的安全验证模型如图 2 所示。验证过程中需要 3 个参与方，被验证信标节点 u、第三方信标节点 t、验证信标节点 v，其中要求验证信标节点 v 是安全可信的。

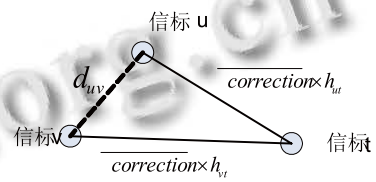

图 2　信标间距约束的安全验证

信标间距约束的安全验证过程分为以下三个阶段：

1) 首先，验证信标节点 v 与第三方信标节点 t 收到被验证信标节点 u 发送的位置信息 (x_u,y_u)。验证信标节点 v 自身位置信息与接收到的验证信息 (x_v,y_v)，利用式（1）计算其与被验证信标节点 v 之间的欧式距离 d_{uv}。

$$d_{uv}=\sqrt{(x_u-x_v)^2+(y_{u-}y_v)^2} \tag{1}$$

2) 第三方信标节点 t 利用式（2）-（4）计算其与验证信标节点 v、被验证信标节点 u 之间的跳段距离

d_{ut}、d_{vt}。其中，n 为网络中信标节点的个数，$correction_i$ 为单个信标节点计算的平均单跳校正值，$\overline{correction}$ 为各信标节点校正值的均值。

$$\overline{correction}=\frac{1}{n}\sum_{i=1}^{n}correction_i \tag{2}$$

$$d_{ut}=\overline{correction}\times h_{ut} \tag{3}$$

$$d_{vt}=\overline{correction}\times h_{vt} \tag{4}$$

3) 参与验证的三方信标节点利用式（5）进行信标间距约束验证。为了评价被验证的结果，此处引入评分机制来量化验证的结果，设被验证信标 u 的量化分值 m 初始值为 10 分。若被验证信标节点 u 通过 1 组式（5）的验证，则被验证信标节点 u 的 m 加 1 分，即 m=11；若有 1 组验证不满足式（5），则被验证信标节点 u 的 m 减小 1 分，即 m=9，以此类推。经过若干组验证，将验证最终的得分结果保存于被验证信标节点 u 的信任列表中。验证结束，若被验证信标节点的量化分值 $m\geq\alpha$（α 为容忍分值），将其视为可信信标；若被验证信标节点的量化分值 $m<\alpha$ 则被视为恶意信标移除出网络。

$$\begin{cases}\left|d_{vt}+d_{ut}\right|>d_{uv}\\ \left|d_{vt}-d_{ut}\right|<d_{uv}\end{cases} \tag{5}$$

3.2 多信标校正值验证

经过上述信标间距约束的安全验证，恶意信标节点被检出并移除出网络，信标节点的比例下降，势必造成算法定位精度的下降。信标比例下降，各个信标节点之间的空间分布差异较大，未知节点到各信标节点的距离用单一的信标节点的平均单跳校正值来衡量显然将带来较大的误差，且少数未被检出的残余恶意信标校正值也可能被对定位产生影响。本文采用多信标校正值权衡的策略优化定位算法，进一步提高定位的安全性。

未知节点随机选取 3 个或 3 个以上的参考信标节点作为定位信标节点。未知节点计算与该定位信标节点的距离时根据式（6）-（7）计算的平均单跳校正值，利用式（8）计算它们之间的距离。

$$\alpha_i=m*\beta\ /h_i^2 \tag{6}$$

$$correction=\sum_{i=1}^{n}\alpha_i c_i \tag{7}$$

$$d_{ij}=correction\times hop_{ij} \tag{8}$$

式（6）中，h_i 为待测节点与网络中各信标节点之间的跳数值，α_i 为依跳数计算的权值，m 为安全验证阶段定位信标节点的量化分值，β 为调和系数，其目的是使 $\sum_{i=1}^{n}\alpha_i=1$；式（7）中，correction 为待测节点最终接收的平均单跳校正值，c_i 为网络中各信标发送的平均单跳校正值。式（8）中，d_{ij} 为待测节点与该定位信标节点之间的估算距离，hop_{ij} 为恶节点与该定位信标节点之间的跳数值。

未知节点与定位信标节点之间跳数值 h_i 越小，量化分值 m 越高，该定位信标节点的平均单跳校正值的权值越大，即离未知节点较近的并且信任度较高的信标节点发送的校正值将被赋予最大的权值。多信标权衡计算所得的平均单跳校正值综合考虑了整个网络情况，使得待测节点计算与较远的信标节点的距离更接近于实际的距离，同时减小了残余恶意信标节点可能作为定位信标节点给未知节点发送错误的平均单跳校正值对定位结果带来的影响。

4 仿真和性能分析

为了检验安全策略的性能，本文在 MATLAB7.0 的平台上进行了仿真对比分析。在 500×500 的仿真区域内，随机分布 200 个网络节点，其中信标节点的比例为 20%，即信标节点数为 40。节点的射频通信半径 R=100。通过改变恶意信标节点的个数来改变恶意信标节点比例，即在被攻击信标节点数占总信标节点的比例分别为 5%、10%、15%、20%、25%、30%。为了更客观地评估该方案的可行性，每个仿真场景运行 10 次，并将每个场景的运行结果取平均值作为实验数据。定位误差定义为未知节点经定位算法的估算坐标位置与其实际坐标位置间的距离与节点的通信半径值的比值，假设未知节点 i 的真实的位置坐标为(x_i,y_i)，经节点定位算法定位所得的位置坐标为$(\hat{x}_i,\hat{y}_i)$，传感器节点的射频通信半径值为 R，则定义未知节点 i 的定位误差 $\delta_i=\frac{\sqrt{(x_i-\hat{x}_i)^2+(y_i-\hat{y}_i)^2}}{R}$。恶意节点的位置坐标信息在仿真区域中随机产生，并与其真实位置信息差距在 R 以外，即：$E=\sqrt{(x_r-x_d)^2+(y_r-y_d)^2}\geq R$，其中恶意节点的真实位置坐标信息及虚假位置坐标信息分别为：(x_r,y_r)和(x_d,y_d)。仿真过程中，每组信标间距约

束的安全验证随机选取 5 个第三方信标节点 t，信标节点的容忍分值$\alpha=8$，若被验证信标节点的量化分值$m\geq 8$，则将其归类为可信信标节点，否则为恶意信标节点。

图 3 是不同比例的被攻击的信标节点的条件下，网络中可定位节点的比例结果。从图中可以看出无安全机制的 DV-Hop 定位算法与本文算法中的 DV-Hop 定位算法在随着被攻击的信标节点比例的增大，网络中可定位的节点比例均在减小，但是在相同的被攻击信标节点比例下，本文的 DV-Hop 定位算法的可定位节点比例比无安全机制的 DV-Hop 定位算法要高。由于随着被攻击的信标节点比例的增大，无安全信标机制的 DV-Hop 定位算法将使未知节点周围出现恶意信标节点的比例增大，在自身定位过程中参考恶意信标节点的位置信息概率也越大，这就会使节点在自身定位过程中计算出的位置坐标信息不出现负数且没有超出仿真区域，使网络中可定位的节点比例下降。而有安全信标机制的DV-Hop定位算法则把恶意节点剔除，这使可参考的信标节点比例下降，使网络中可定位的节点比例下降的主要原因。

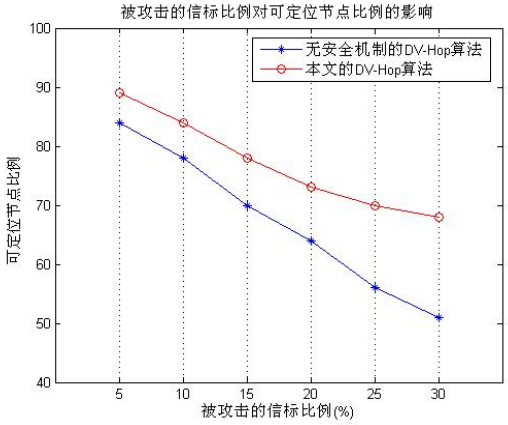

图 3 被攻击的信标节点比例对可定位节点的影响曲线

图 4 是在上述实验参数环境下网络中不同比例被攻击的信标节点对未知节点定位误差的影响曲线。从图中可以看出，随着被攻击的信标节点比例的增大，无安全机制的 DV-Hop 定位算法与有安全信标机制的 DV-Hop 定位算法的定位误差均在增大，但是在相同被攻击的信标节点比例下，有安全信标机制的 DV-Hop 定位算法的定位误差比无安全机制的 DV-Hop 定位算法小。由于随着被攻击的信标节点比例的增大，有安全信标机制的 DV-Hop 定位算法将排除越来越多的恶意信标节点，相当于整个网络中可信的信标节点总数在下降，即可参考的信标节点比例下降，这是使有安全信标机制的 DV-Hop 定位算法的定位误差增大的主要原因。

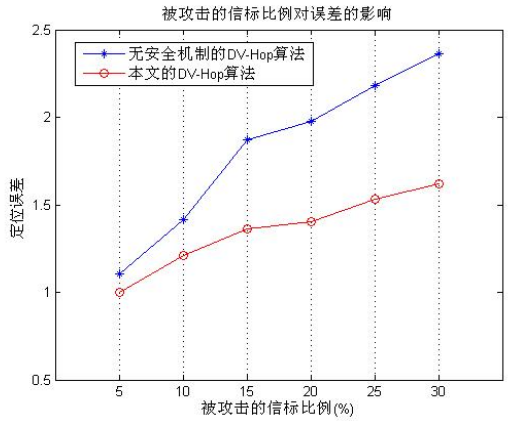

图 4　在不同被攻击信标比例下节点的定位精度

5　结论

本文根据恶意信标节点的位置欺骗攻击模型，分析了该攻击方式对 DV-Hop 算法的影响，在此基础上提出了一种抵抗恶意信标节点的安全优化定位算法，通过信标之间的距离约束验证与多信标校正值权衡的策略，尽可能减小信标节点位置欺骗攻击对定位的影响，提高定位的安全性。仿真实验表明，该安全算法有效地提高了可定位节点的比例，减小了恶意信标节点对定位精度的影响。

参考文献

1 叶阿勇.无线传感器网络节点安全定位[博士学位论文].西安:西安电子科技大学,2009.

2 Liu D, Ning P, Du W. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. Proc. of International Conference on Distributed Computing Systems. Columbus: IEEE, 2005. 609–619.

3 许金红.无线传感器网络中恶意节点的检测和定位策略的研究.长沙:中南大学,2009.

4 Liu D, Ning P, Du WK. Attack-resistant location estimation in sensor networks. Proc. of IPSN 2005, Los Angeles: IEEE Computer Society, 2005. 99–106.

5 Srinivasan A, Teitelbaum J, Wu J. Distributed Reputation-based Beacon Trust System. Proc. of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, IEEE Press, 2006. 277–283.

6 钟进发.无线传感器网络节点定位算法的研究[硕士学位论文].福州:福建师范大学,2010.