第35卷 第12期 计 算 机 工 程 2009年6月
Vol.35 No.12 Computer Engineering June 2009
·安全技术· 文章编号：1000—3428(2009)12—0117—03 文献标识码：A 中图分类号：TP309

基于对称密码的无线传感器网络安全定位

靖 刚[1,2]，吴俊敏[1,2]，徐宏力[1,2]，黄刘生[1,2]
(1. 中国科学技术大学计算机科学与技术系，合肥 230027；
2. 中国科学技术大学苏州研究院，苏州 215123)

摘 要：伪装攻击通过恶意的锚节点向网络中发布虚假位置信息从而对定位应用进行攻击。针对上述问题，考虑无线传感器网络节点能量受限的特性，提出一种基于对称密码加密的认证方案来防御伪装攻击。实验结果表明，在伪装攻击存在的情况下，该方案能够使加权质心算法的定位误差在1 m之内的概率由40%提高到70%，从而保证定位的正确性。

关键词：无线传感器网络；伪装攻击；安全定位

Secure Localization Based on Symmetric Cryptography in Wireless Sensor Networks

JING Gang[1,2], WU Jun-min[1,2], XU Hong-li[1,2], HUANG Liu-sheng[1,2]
(1. Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230027;
2. Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou 215123)

【Abstract】This paper presents a security threat model called impersonating attack model. In this model, the malicious beacons supply forged location information to the regular sensors, so as to attack the location applications. Since sensor nodes are power and computational capacities limited, a scheme based on symmetric cryptography is proposed to defense against impersonating attack. Experimental results show that, even in the presence of impersonating attack, the scheme can decrease the cumulative localization error of Weighted Centroid Algorithm. The probability which the localization error is within 1 m can be improved from 40% to 70% with the scheme.

【Key words】Wireless Sensor Networks(WSN); impersonating attack; secure localization

1 概述

随着现代通信技术和计算机微电子技术的飞速发展，无线传感器网络已成为当前研究的热点领域。而节点定位问题是传感器网络的关键技术之一。目前，在节点定位方面，提出了很多既有实用价值又有理论研究意义的定位算法，这些定位算法总体上可以分为两大类:基于测距的和无需测距的。典型的基于测距的算法有：TOA(Time of Arrival), TDOA (Time Difference of Arrival), AOA(Angle of Arrival)等；典型的无需测距的算法包括质心算法[1]、加权质心算法[2]等。但是这些算法性能的评估是在假设网络中所有的节点都是合法节点的前提下进行的。

在已有的定位算法中，定位系统本身并不提供身份认证和加密机制来验证节点的合法性。对于无需测距的算法，如果在节点定位的过程中外部恶意节点伪装成锚节点，或者锚节点之间的通信链路受到恶意节点的破坏，其结果势必会对节点的定位精度产生很大的影响。伪装成锚节点的恶意攻击也叫伪装攻击，文献[3]提出了一种基于锚节点位置约束的方法来检测恶意锚节点。

本文研究了无需测距的定位算法中存在的伪装攻击问题，并利用对称密码加密与认证的方案解决了该问题。该方案能够在伪装攻击存在的环境中，对节点进行安全定位。

2 安全威胁模型

无线传感器网络是由大量廉价的传感器节点组成的，这些节点通常放在无人看管的环境下，因此，攻击者很容易在节点的分布区域中加入外部恶意节点，从而扰乱整个网络系统的正常运行。假设节点在物理上是安全的，即节点不会遭到人为的破坏。

在定位算法进行定位的过程中，由于节点之间主要以广播的方式进行通信，因此外部恶意节点可以伪装成网络中的锚节点，向网络中广播伪造的位置消息。未知节点在收到伪造的位置消息后，就会产生错误的定位估计(定位误差扩大或者减小)。这种安全威胁称为伪装攻击。

图1描述的是利用加权质心算法定位时得到的一个定位场景。在该场景中，位于(2,5)处的攻击节点伪装成位置(0,0)处的锚节点，向网络中广播含有位置(0,0)的消息，结果造成定位误差由0.766 m扩大到1.078 m。另外，改变伪装锚节点的发包频率也会对节点的定位误差产生较大的影响。如图2所示，1 s/包是无伪装锚节点时得到的定位误差，0.5 s/包和1.5 s/包是有伪装锚节点时得到的定位误差。由图2可以看出，伪装锚节点的发包频率越小，节点的定位误差波动就越大。这主要是因为伪装锚节点的发包频率越小，相同时间内它发出的伪造消息就越多，被未知节点接收到的概率就会越大。

基金项目：国家“973”计划基金资助项目“无线传感器网络应用示范系统”(2006CB303006)；国家“973”计划前期研究专项基金资助项目“多层结构的移动传感网络理论、关键技术及动态监测仿真研究”(2007CB316505)

作者简介：靖 刚(1981－)，男，硕士研究生，主研方向：无线传感器网络；吴俊敏，讲师；徐宏力，博士后；黄刘生，教授、博士生导师

收稿日期：2008-11-07 **E-mail：**gjing@mail.ustc.edu.cn

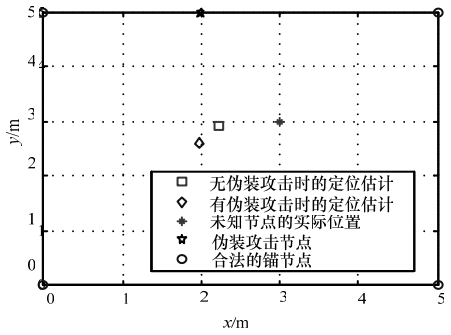

图 1　有无伪装攻击定位场景

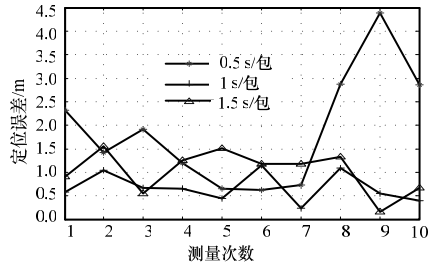

图 2　伪装锚节点的发包频率对定位误差的影响

3　安全定位算法设计

3.1　算法设计

由于伪装攻击主要通过向网络中广播伪造的位置消息来影响节点定位的精度，因此可以采用加密与认证的机制对所有接收到的消息进行认证，通过认证的消息则接收，没有通过认证的消息直接丢弃。

整个算法由以下 3 步组成：

(1)网络中合法的锚节点在发送广播消息之前计算自己的私钥和 hash 认证码[4]，并用自己的私钥对 hash 认证码进行签名，然后使用网络中的全局共享密钥对附有签名的消息进行加密，并将加密后的消息广播到网络中。

(2)网络中的其他节点在接收到广播消息之后，先使用全局共享密钥对消息进行解密，然后使用解密后消息中的节点标识符和本地全局共享密钥计算源节点的私钥，并利用私钥验证签名，再使用解密后的消息产生的 hash 认证码验证源节点附上的认证码。

(3)利用认证通过的消息进行定位计算，输出定位结果。对于没有通过认证的消息，可以直接丢弃。

对消息进行加密可以使用对称密码(如 DES, RC5)或公开密码(如 RSA, ECC)[4]。尽管文献[5]中已经在 Mica2 平台上实现了公钥加密算法 ECC，但是，由于节点的电池能量和计算能力有限，公钥加密不适用于当前的无线传感器网络。而对称密码无论是在电池能量还是计算能力方面，都比较适合无线传感器网络，比如文献[6]的方案已经在节点上实现了对称加密算法 Skipjack 和 RC5。

上述防御措施可以形式化描述如下：假设 K 是网络中的全局共享对称密钥，$E_K(m)$表示用密钥 K 对待发送的消息 m 进行加密。$D_K(M)$表示用密钥 K 对接收到的消息 M 进行解密。N 表示网络中的节点个数，其对应的节点标识符分别为 ID_1, ID_2, …, ID_N。$m_i(1\leqslant i\leqslant N)$表示节点 i 产生的待发送消息，其对应的 hash 认证码为 $hash(m_i)$。$M_i(1\leqslant i\leqslant N)$表示节点 i 收到的消息，它对应的 hash 认证码为 $hash(M_i)$。$K_i(1\leqslant i\leqslant N)$表示节点 i 的私钥，它可以通过函数 $f(ID_i, K)$计算得到。$f(M_i)$表示利用消息 M_i 进行定位计算。则整个算法伪代码如下：

```
for each mi do
    Ki = f(IDi,K) ;
    EK(mi|| EKi(hash(mi))), ;
// ||表示串联操作
end for
for each Mi do
DK(Mi) ;
Ki = f(IDi,K) ;
if(hash(Mi)= DKi(DK(Mi)中的 hash 码))
   f(Mi);
else
  discard Mi;
end if
end for
```

3.2　算法的正确性

网络中合法的节点由于拥有全局共享密钥，因此可以解密并且认证通过其他合法节点发来的定位消息，而丢弃未通过认证的伪装锚节点发出的伪造消息。

伪装节点由于不知道全局共享密钥以及合法节点私钥的生成方式，因此不能解密收到的定位消息从而获得有关合法节点的任何信息。所以，该算法是正确的。

3.3　算法分析

由于不同的定位系统所要求的安全等级和定位精度各不相同，因此该算法的时间和空间复杂度取决于所使用的加密算法、hash 算法和定位算法三者的时间和空间复杂度。另外，全局共享密码是预先加载到节点上的，而节点的私钥是通过计算得到的，所以，该算法不会额外增加定位系统的通信开销，这一点对于能量受限的传感器节点来说十分重要。因为节点在物理上是安全的，节点不会被攻击者捕获，所以攻击者不能通过捕获节点的方法来获得存储在节点上的全局共享密钥。即使全局共享密钥泄漏，由于不知道节点私钥的生成方式，因此攻击者仍然很难对定位系统造成威胁。

该算法由于对所有收到的消息进行验证，因此即使网络中存在伪装攻击节点，它所伪造的位置消息在被传递到超过 1 跳邻居之外的节点接收之前会被完全过滤掉。所以，该算法可以保证在伪装攻击存在的场景下，定位算法不会丢失定位精度。

4　实验

4.1　实验描述

实验以加权质心算法为例研究伪装攻击防御措施的有效性。实验中所用到的节点端测试程序是基于 TinyOS 1.1.10 系统在 MicaZ 平台上利用 NesC 语言开发的，其中，RF 能量级设为 TXPOWER_MAX。实验是在中国科技大学苏州研究院亲民楼 303 学生机房进行的。实验中使用了 crossbow 公司生产的 7 个 MicaZ mote 节点，其中有 6 个合法节点和 1 个伪装攻击节点。4 个合法的锚节点摆放在一个 5 m×5 m 正方形的 4 个顶点处。节点坐标分别为 $B_1(0,0)$, $B_2(5,0)$, $B_3(5,5)$, $B_4(0,5)$，B_0 作为基站通过串口与定位服务器相连，B_{10} 作为未知节点。伪装攻击节点 B_1'坐标为(2,5)。然后将这个正方形细分为 25 个 1 m×1 m 的小方格，随机选取 10 个格点作为未知节点的位置，进行安全定位计算。

在算法实现的过程中，全局共享密钥 K 可以随机选择密钥空间内的一个常数。加密算法使用加密速度较快的 RC5 算法。节点的私钥 K_i 由伪随机函数[4]生成，认证码使用简单 Hash 函数[4]生成。算法实现可分为 2 个阶段：第 1 个阶段是定位消息的加密与认证阶段。该阶段周期为 2 s，记录下未知节点

接收到的各个锚节点发来的定位消息包，在每个格点处共收集 50 个定位消息包。第 2 个阶段是利用加入伪装攻击防御措施的加权质心算法对未知节点进行安全定位。

4.2 实验结果及分析

图 3 是在有攻击节点存在的环境下，加入防御措施和没有防御措施的定位误差及无恶意节点时的定位误差比较。由图中可以看出，在多数情况下，有伪装攻击节点时的定位误差比没有时的定位误差扩大了许多，只有少数情况下定位误差减小了。而在加入防御措施后，节点的定位误差和没有攻击节点时基本相同。图 4 是对应的定位误差的累计概率分布。

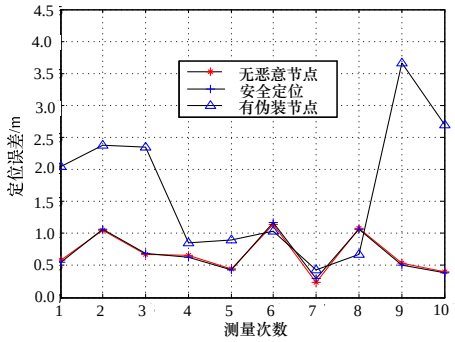

图 3 定位误差比较

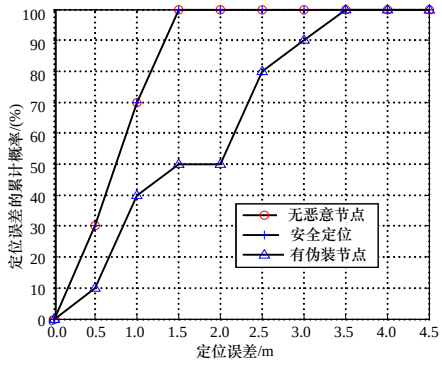

图 4 定位误差的累计概率分布

由图 4 可以看出，在存在伪装攻击的环境中，节点的定位误差在 1 m 之内的概率在 40%以下，而在加入防御措施后，达到这种精度的概率在 70%左右。

5 结束语

本文针对无线传感器网络定位算法中存在的伪装攻击，提出了一种基于对称密码加密的防御措施。实验结果表明，在伪装攻击存在的环境中，该防御措施可以在不失算法定位精度的情况下，对节点进行安全定位。由于传感器节点通常分布在无人照看的环境下，一旦节点被攻击者捕获，存储在节点上的所有信息都会被攻击者得到，因此如何在节点被捕获的情况下仍能安全定位将是下一步工作研究的重点。

参考文献

[1] 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.

[2] Shen Xingfa, Wang Zhi, Jiang Peng, et al. Connectivity and RSSI Based Localization Scheme for Wireless Sensor Networks[C]//Proc. of IEEE 2005 International Conference on Intelligent Computing. Berlin, Germany: Springer-Verlag, 2005: 578-587.

[3] Liu Donggang, Ning Peng, Du Wenliang. Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks[C]//Proc. of the 25th Int'l Conf. on Distributed Computing Systems. Washington, USA: IEEE Computer Society Press, 2005.

[4] Stallings W. Cryptography and Network Security Principles and Practices[M]. 4th ed. [S. l.]: Prentice Hall, 2005-11.

[5] Wang Haodong, Sheng Bo, Li Qun. Elliptic Curve Cryptography Based Access Control in Sensor Networks[J]. International Journal of Security and Networks, 2006, 1(3/4): 127-137.

[6] Karlof C, Sastry N, Wagner D. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks[C]//Proceedings of ACM SenSys'04. Maryland, USA: [s. n.], 2004.

编辑 张正兴

(上接第 116 页)

返回到自定义的过滤接收函数。因此，要获得底层 SPI 的接收数据大小的信息，如果用户进程是使用重叠 I/O 方法发出的 Winsock 接收调用，需要先保存原来的 Winsock 调用传递参数信息，定义自己的回调函数完成例程，再转发给底层处理。这样在转发给底层处理时就告诉了操作系统需要控制权最终返回。

5 结束语

本文目标是实现一个适用于所有 Window 平台的个人防火墙系统，由于 TDIS 和 NDIS 的包过滤技术路线都不能适用于所有 Windows 平台，因此从项目目标来看，选用 SPI 是合适的。笔者使用 SPI 实现了一个人防火墙系统 MyFilter 1.0，实验表明其具有较好的包过滤处理性能。但可以看到，SPI 和 TDI 都有被“旁路”的可能，而只有 NDIS 能从底层截获所有的网络通信数据包解决旁路隐患。因此，一个真正可商业化的个人防火墙系统必须同时具备高层包过滤和 NDIS 底层包过滤的“双截获”方案才能达到理想的效果，即既能在高层包过滤充分获取访问进程信息，又能在在底层采用 NDIS 解决旁路的隐患。笔者正在对 SPI+NIDS 的复合技术路线进行技术验证，但这样的个人防火墙系统不能适用于所有 Windows 平台。

参考文献

[1] 黄允聪，严望佳. 计算机网络安全工具[M]. 北京: 清华大学出版社, 1999: 35-41.

[2] Tanenbaum A S. 计算机网络[M]. 4 版. 北京: 清华大学出版社, 2004: 60-62.

[3] Goncalves M. Firewalls: A Complete Guide[M]. 北京: 机械工业出版社, 2000: 77-79.

[4] Zwicky E D, Cooper S, Chapman D B. Building the Internet Firewall[M]. 2 nd ed. [S. l.]: McGraw-Hill, 2003: 90-95.

[5] 刘鹏远. Windows 下个人防火墙的研究与实现[D]. 昆明: 云南大学, 2005.

[6] 王树华，周利华. 基于 Windows 2000 平台的防火墙技术研究与实现[J]. 微机发展, 2004: 14(5): 78-80.

[7] 戚鹏飞. Windows 下的个人防火墙——网络数据包拦截技术概览[EB/OL]. (2007-02-25). http://blog.csdn.net/welkint/archive/2007/02/25/1513624.aspx.

编辑 张正兴