



WSN 中基于周期性超宽带距离信息的女巫攻击检测

张衍志, 叶小琴

(四川工程职业技术学院, 四川 德阳 618000)

摘要: 针对无线传感器网络易受多种网络攻击和节点妥协的问题, 提出一种基于周期性超宽带距离信息的女巫攻击检测的完整系统。首先进行相邻节点间的测距和 hello 数据分组的交换, 然后采用局部估算方式构建距离估计表格, 并使每个节点均含有这种表格。接着, 在网络中周期性地对每个节点独立执行多个距离匹配检查。最后, 当合法节点在至少 2 个不同节点之间找到了距离匹配时, 就发出警报废除女巫节点。如果不存在距离匹配, 节点继续正常操作。模拟实验配备 IEEE 802.15.4 对等传感器网络, 实验结果证明了提出的系统可以容忍并发女巫攻击数量的变化, 也可以成功处理同时发生的、可延展的女巫攻击。另外发生假警报的概率非常小, 整个网络性能及其一致性没有受到影响。

关键词: 无线传感器网络; 超宽带; 女巫攻击; 距离估计表格; 距离匹配

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016198

Detection of sybil attacks based on periodic ultra wide band distance information in WSN

ZHANG Yanzhi, YE Xiaoqin

Sichuan Engineering Technical College, Deyang 618000, China

Abstract: Concerning the problem that wireless sensor network is vulnerable to many kinds of network attacks and compromise of nodes, a complete detecting system of sybil attack based on periodic ultra-bandwidth distance information was proposed. Firstly, the distance between the adjacent nodes was ranging and the hello data packet was exchanged. Then, the distance estimation form was constructed by local estimation, and the form was contained in each node. Meanwhile, multiple distance matching check was periodically executed for each node in the network. Finally, when there was the distance matching between the legitimate node at least two different nodes, it would give an alarm and discard the sybil nodes. If there was no distance matching, the node continued normal operations. IEEE 802.15.4 peer to peer sensor networks were adopted in the simulation experiments. Experimental results show that the proposed system not only can tolerate changes in the number of complicated sybil attacks, but also can successfully deal with the occurrence of complicated, malleable sybil attack. In addition, the probability of false alarm is very small, the entire network performance and its consistency are not affected.

Key words: wireless sensor network, ultra wide band, sybil attack, distance estimation form, distance matching

1 引言

近些年,无线传感器网络^[1](wireless sensor network, WSN)具有许多特征,如自组织性、灵活性、容错性、高传感保真度、低成本和快速发展性^[2],在没有任何集中基础设施的情况下,这些特性使 WSN 成为快速、动态提供网络服务(如安全报文宣传和时间通知)的理想候选。在假设支持该技术的情况下,为了确保众多应用程序的安全,WSN 领域中各区域都需要认真研究和实践。毫无疑问,安全性是网络设计中需要首先处理的关键元素之一^[3]。

WSN 易受攻击,其无人值守和广播性质使其容易受到各种攻击和节点妥协的影响。女巫攻击就是其中常见的一种,女巫攻击一般定义为:非法具有多重身份的恶意设备^[4,5]。现有许多主动或被动的方法对抗女巫攻击,这些方法可分为 3 个主要范畴:基于身份的方法^[6,7]、基于位置验证的方法^[8-10]和基于视觉的方法^[11,12]。

(1) 基于身份的方法

即通过限制有效节点信息的生成来缓解女巫攻击。该方法依赖于中央服务器分配的安全 ID。参考文献[6]提出一种基于身份证明的方案来处理 WSN 中的女巫攻击,每个网络节点都有唯一的认证来保护其身份,采用散列树来应用该认证方案。然而,该方案计算成本非常高,其计算成本主要集中在计算时延以及交流节点间的信息交换负荷。参考文献[7]提出一种监测技术,每个节点周期性记录接收到的不同身份集,然后使用统计分析来检测女巫攻击。该方案背后的原理在于合法节点常随着网络移动,而女巫攻击留在一起。但是恶意节点可能应用不可预知的移动模式并且不容易被发现。

(2) 基于位置验证的方法

基于每个节点在任何给定时间内都只能有一个位置(物理位置)的事实,通过使用距离测量和三角测量检查每个身份的位置^[8]。参考文献[9]提出了一种基于接收信号强度指示器的方法来预防女巫攻击。一组可信传感器节点起到了探测器的作用。根据接收到的信息,该探测器通过监测接收的信号功率估算信息发送器的位置。如果一组身份都存在于相同区域内,那么探测器就认为该节点是女巫节点。参考文献[10]提出一种基于位置的密钥(location based key, LBK)的概念。每个节点拥有一套私有密钥来保护其身份和位置。在任何可能的节点对之间采用了共享密钥。然后使用一种认证方案阻止恶意活动。该方案可以造成恶

意节点不能完成与其他节点的认证,从而解决每个潜在的女巫攻击。总之,基于位置的方法是 WSN 中比较有前途的女巫攻击检测技术。然而,这类方法依赖无线电信号性能,易受干扰,可能会显著降低其检测精度。

(3) 基于视觉的方法

通过可视化方法来监督并检测 WSN 中的女巫攻击。该领域还处于初始阶段,参考文献[11]使用多视图的方式获得网络拓扑信息并显示与女巫攻击的数据相关性。参考文献[12]提出一种综合方法,通过可视化和分析多个重新排序拓扑的模式来检测 WSN 中的女巫攻击。这些方法的不足是需要更多可视化工作和人机交互。

与上述攻击检测系统(attack detecting system, ADS)不同,本文方法基于超宽带(ultra wide band, UWB)^[13]技术,周期性地检查节点间的距离,并给出一些规则,即基于周期性超宽带距离(periodic ultra wide band distance, PUWBD)的女巫攻击检测系统,其优势是可以直接适用于 IEEE 802.15.4 兼容 WSN 操作。其主要贡献有:提出了一种通信开销低的女巫攻击检测系统,可以防御同时具有偷窃和伪造身份的女巫攻击;介绍了一种分布式的基于 UWB 测距的检测算法,能够检测恶意节点和女巫节点,并将其列入黑名单而不参与集中操作,即分布式操作。

2 PUWBD 异常检测系统

2.1 假设和攻击模型

本文考虑了一种包含了 M 个传感器节点的基于 IEEE 802.15.4 UWB 的 WSN。如图 1 所示,这些节点均匀分布于区域 E 内,节点静止,且不知道自己的位置。此外,假设节点通过无线电通道与其他节点进行通信并且在半径为 R 的圆形区域中广播。当节点传播信息时,该信息只能由那些在发送器通信范围内并指定为“相邻节点”或“邻居节点”接收。此外,本文假设不完全信任任何节点,这是不存在分布式信任模型,大量合法节点可能会针对女巫攻击进行篡改和重组。

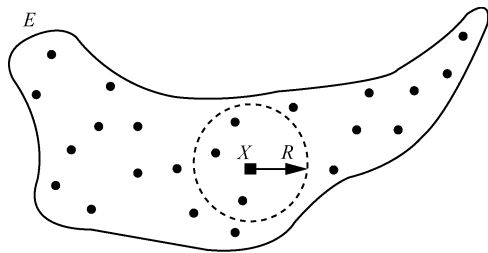


图 1 无线传感器领域



根据参考文献[14],可以使用3种维度来代表女巫攻击:通信、身份、参与。通信涉及女巫节点如何引入网络合法节点中。存在两种可行的通信方法:直接(女巫节点与合法节点通信)和间接(合法节点不直接与女巫节点通信)。

身份维度代表了1种模型,通过该模型女巫节点可以获得身份。一般有两种可能的方式:偷盗身份和伪造身份。即女巫节点可以通过冒充合法节点而偷取身份以及伪造任意新身份。最后,女巫节点参与到网络中合法节点之间的通信中。这些节点可以同时或非同时参与其中。同时参与时,恶意节点一次使用所有身份参与,而在非同时参与模式中,恶意节点在一定时期内显示大量身份。

根据上述范畴,本文考虑了具有偷盗和伪造身份的直接、同时的女巫攻击。这种攻击的典型范例如图2所示。被俘节点称为恶意节点,其他节点即合法节点。攻击模型假设恶意节点伪造多种新身份,其创建的每个实体都有一个身份。恶意节点的主要任务是欺骗合法节点相信其有邻居。然而,由于女巫节点并不真实存在,所以女巫节点的存在可能严重干扰许多网络协议甚至使其瘫痪。

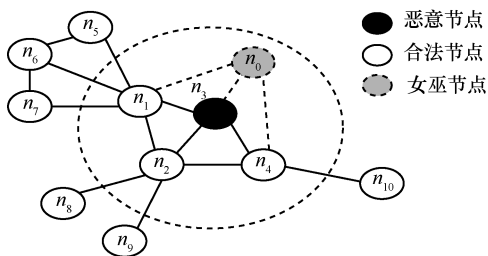


图2 具有10个节点的WSN的拓扑结构

2.2 详细描述

一般地,异常检测器使用预定义的规则将数据点划分为异常或正常。在监测网络时,适当选择这些规则并应用于监测数据。如果规则定义异常为满意,即宣布其为异常。在PUWBD中,潜在检测器通过以下4步检测WSN中的女巫攻击。

步骤1 邻居发现阶段。包括相邻节点之间的测距,并允许hello数据分组(也称为指向标)的交换,用于测距估算的是标准数据分组,唯一不同的是叫做“测距比特”的PHY数据头中特定比特的值^[15]。

步骤2 每个节点包含了局部计算的距离估算表格,即到每个相邻检测节点的距离 d_{ij}^e, d_{ij}^s 表示节点 n_i 测量到的节点 n_i 和 n_j 之间的估算距离。然而,距离估算并非没有误差。本文使用 ε 表示测距误差,由于测距通信的无线特

征和潜在PHY的不完美,或者由于恶意节点的距离减小或增加攻击^[13]。因此,用 d_{ij}^a 表示节点 n_i 和 n_j 之间的真实距离。显然, $d_{ij}^e - \frac{\varepsilon}{2} \leq d_{ij}^a \leq d_{ij}^s + \frac{\varepsilon}{2}$ 表示节点 n_i 和 n_j 的平均水平,其中, $i, j \in M$ 。表1所示为图2描述的网络拓扑结构中节点 n_2 的测距。

表1 节点 n_2 的测距

	n_0	n_1	n_3	n_5	n_6	n_7
n_2	d_{20}^e	d_{21}^e	d_{23}^e	d_{25}^e	d_{26}^e	d_{27}^e

步骤3 网络中的每个单一节点独立执行多个距离匹配检查,即计算节点 n_i 与其邻居列表中包含的节点 n_j 和 n_k 的每个可能部分的距离差,即对于所有 $j, k \neq i, 1 \leq j, k \leq M$ 。

如果 $|d_{ij}^e - d_{ik}^e| < \varepsilon$ 则报警,否则 $|d_{ij}^e - d_{ik}^e| \geq \varepsilon$ 继续正常模式,上述规则表明假如节点 n_i 发现两个其他独立节点(用 n_i 和 n_k 表示),其距离不同且少于 ε ,那么节点在执行距离检测时,将节点 n_j 和 n_k 列入黑名单。显然,如果两个距离匹配节点 n_j 和 n_k 为合法传感器节点,那么这种假设会产生假警报。

这里,需要着重说明的是该算法的步骤3是循环步骤,即周期性进行距离检查。每个节点执行基于UWB测距的女巫攻击检测算法的周期依赖于每个节点在其周围发现新邻居的频率。节点每次寻找已有邻居或新邻居时都要重新运行距离检查。这4个步骤确保了新增邻居之间的距离检查是最新的,并且每个其他现存节点都在邻居列表中。

步骤4 当合法节点在至少两个不同节点之间找到了距离匹配时,就会发出警报试图废除女巫节点。在废除女巫节点过程中,合法节点即PUWBD—能力检测器,向基站发送警报信息使网络管理员能够采取对策。也将这些节点列入黑名单中,从而避免将这些节点添加到邻居列表中。如果不存在距离匹配,那么节点继续正常操作。在该操作中,节点在其邻居之间发送并接收网络数据分组来实现分配到的任务。

提出的基于UWB测距的女巫攻击检测算法是完全分布式的,即数据收集、监测和检测过程都是在大量网络位置上执行。这种架构显然意味着所有网络节点都能够运行提出的异常检测算法。此外,节点之间不需要合作或信息共享来废除恶意节点。因此,没有因为检测目的而产生的通信开销。最后,在检测异常时,使用了局部审计数据,每个

节点都作为独立的异常检测系统 (anomaly-based detection system, ADS) 工作, 也负责针对其自身的攻击。算法 1 给出了基于 UWB 测距的女巫攻击检测算法的不同阶段。

算法 1 基于 UWB 测距的女巫攻击检测

初始化节点的黑名单列表

为安排邻居发现阶段, 初始化定时器

for 每次邻居发现—相关定时器到期 do

for 网络中每个节点 $i, i \in M$ do

步骤 1 与每个邻居节点交换测距—激活信标

步骤 2 构建包含每个检测邻居节点 j 的测距误差 $\{d_{ij}^e\}$ 的表格, $j \in M$

步骤 3 执行距离检查

for 邻居列表中每个可能的节点对 do

if $|d_{ij}^e - d_{ik}^e| < \varepsilon, 1 \leq j, k \leq M, k \neq i$ then

通过将节点 j, k 插入 NBL 来发出警报废除节点 j, k

else

继续常规操作

end if

end for

end for

end for

3 分析

3.1 问题公式化

为简单起见, 本文假设传感器节点覆盖了整个区域。配置每个传感器节点来覆盖半径为 R 的圆形通信范围。圆盘形状中节点的通信范围模型如图 3 所示。隐含了离散的圆环形状 (传感器节点位于圆盘的中央)。该圆盘划分为相同宽度 ε 的同心环。

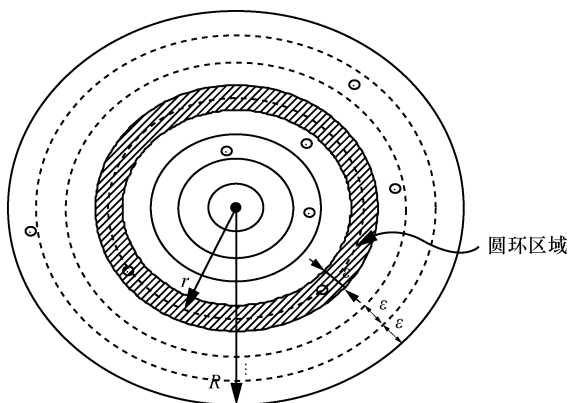


图 3 分析模型

为了不失一般性, 考虑网络节点的子集, 即节点 n_i, n_j 和 n_k , 其中, 节点 n_i 为检测节点, 而节点 $n_j, n_k \neq n_i$ 为节点 n_i 针对女巫攻击而检查的节点。目的是计算两个节点位于同一圆环的概率。节点 n_j 和 n_k 不能共存的区域产生了假警报并形成了圆环形状, 本文将这种概率称为共存区域概率, 产生假警报的核心规则为:

$$|d_{ij} - d_{ik}| < \varepsilon, 1 \leq i, j, k \leq M, k \neq i \quad (1)$$

然后, 本文使用几何概率的概念来建立分析。

3.2 假警报的概率分布

通过计算至少 1 个节点安排至少 2 个节点处于通信半径为 R 的相同圆环中的概率, 推导出发送假警报的概率。当检测到至少 1 对节点处于相同圆环中时, 节点便会发送警报。当在相同圆环内获得 2 个以上节点时也会得到相同结果。

所以, 本文寻求的是至少 1 个节点 n_i 安排至少 2 个其他节点 n_j 和 n_k 处于相同圆环区域内的概率 P , 假设节点 n_i 的通信半径为 R , 且 M 个节点都均匀分散在传感器区域 E 内。通过排除其他概率事件可以推导出至少 1 个事件的概率。因此, 期望的概率计算如下:

$$P = 1 - q^i(0) - q^i(1) - q^i(2) - \dots - q^i(M-1)l^i(M-1) \quad (2)$$

其中, $q^i(0)$ 为节点 n_i 没有邻居的概率; $q^i(1)$ 为节点 n_i 恰好只有 1 个邻居的概率; $q^i(2)$ 为节点 n_i 恰好有 2 个邻居的概率; $q^i(M-1)$ 为节点 n_i 有 $M-1$ 个邻居的概率, 即所有其他节点都是其邻居; $l^i(2)$ 表示在节点 n_i 范围内没有 2 个邻居处于相同圆环内的概率; $l^i(M-1)$ 表示在节点 n_i 范围内没有 $M-1$ 个邻居处于相同圆环内的概率。

式 (2) 的计算需要测定概率分布 $q^i(x)$ 和 $l^i(x)$ 。下面简要进行说明。

3.2.1 节点邻居的概率分布

本节确定恰好具有 x 个邻居的单一节点 n_i 的概率密度函数 (PDF)。考虑到 M 个节点均匀分布于区域 E 的同一传感器领域内, 概率 $q^i(x), 0 \leq x \leq M-1$, 推导如下:

$$q^i(x) = \Pr(X=x) = \binom{M-1}{x} \alpha^x (1-\alpha)^{M-(x+1)} \quad (3)$$

其中, $\alpha \leq 1$ 表示节点 n_j 处于节点 n_i 的通信半径 R 内的几何概率, 其中, $n_i \neq n_j$ 。 α 为:

$$\alpha = \frac{\pi R^2}{E}, \pi R^2 \leq E \quad (4)$$

3.2.2 泛化共存区域概率分布

圆环的宽度为 ε , 节点 n_i 的通信区域半径为 R 。对于



恰好具有 x 个邻居的节点 n_i , 从 M 个邻居中找不到 1 个与 n_i 位于相同圆环内的概率, 用 $O^i(x)$ 表示, 具体形式为:

$$O^i(x) = q^i(x) l^i(x) = \binom{M-1}{x} \alpha^x (1-\alpha)^{M-(x+1)} (1-w)^{x(x-1)/2} \quad (5)$$

将式(5)带入式(2), 概率 P^i 可表示为:

$$\begin{aligned} P^i &= 1 - q^i(0) - q^i(1) - q^i(2) - q^i(3) - \dots - q^i(M-1) l^i(M-1) \\ &= 1 - (1-\alpha)^{M-1} - (M-1)\alpha(1-\alpha)^{M-2} - O^i(2) - \dots - O^i(M-1) \\ &= 1 - (1-\alpha)^{M-1} - (M-1)\alpha(1-\alpha)^{M-2} - \dots - \sum_{w=2}^{M-1} \binom{M-1}{w} \alpha^w (1-\alpha)^{M-(w+1)} (1-w)^{w(w-1)/2} \end{aligned} \quad (6)$$

只有当单一节点执行测距时上述分析才成立。特别是式(6)给出了单一节点引发假警报的概率。然而, 在具有 M 个节点的传感器网络中, 任何节点都可以引发假警报。因此, 本文寻求具有 M 个节点的传感器网络中至少 1 个节点引发假警报的概率。该概率用 p 表示, 计算如下。

引理 1 M 个节点的传感器网络中的假警报概率 $p = 1 - (1-P)^M$, 其中, 区域 E 内每个节点的通信半径为 R , 且其测距过程的平均误差为 ε 。

$1 - P^i$ 表示单一节点没有引发假警报的概率。因此, $(1 - P^i)^M$ 为网络中所有节点都没有引发假警报的概率。按照这种方式, $1 - (1 - P^i)^M$ 表示至少 1 个节点引发假警报的概率。

4 性能评估

4.1 仿真环境

本文使用矩阵实验室中自定义开发的仿真环境来评估提出算法的性能。模拟了配备有 PUWBD 检测器的 IEEE 802.15.4 对等传感器网络。传感器节点 M 在 10~100 中变化, 默认为 50; 均匀分布在传感器运动区域 E 内, E 在 0.5~1 km² 中变化, 默认为 1 km²; 每个节点的通信范围的半径为 R , 在 5~50 m 中变化, 默认为 30 m。最后, 每个节点的平均测距偏差 ε 在 10~100 cm 中变化, 默认值为 30 cm。

4.2 模型验证分析

本节在每个图形中, 标出至少 1 个节点引发假警报的概率, 参数改变分别是: 传感器区域内的传感器节点的数量 M 、通信半径 R 、测距估算误差 ε 、节点密度 $\rho = M/E$ 。

图 4 给出了改变节点数量产生假警报的概率。设置传感器区域为 $E = 1$ km², 所有节点具有相同的通信半径, $R = 30$ m, 以及相同的平均测距误差 $\varepsilon = 30$ cm。节点的数量在 10~90 改变。从获得的曲线中可以发现: 首先, 提出的算法

在假警报产生方面的性能很好, 即使对于大量传感器节点, 该误差仍低于 0.004 5。仿真结果符合解析方程。这两种曲线对于所有节点几乎都相同, 这个事实显示了提出的分析框架的精确度。由于节点数量的增加, 假警报概率也增加。由于节点数量的增加是可预期的, 有可能至少 1 个节点会找到至少 2 个其他节点处于共同的通信范围内。

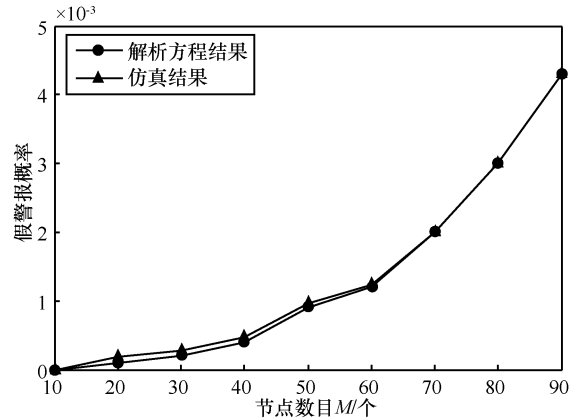


图 4 假警报概率与节点数的关系

图 5 根据通信半径 R 描述了假警报概率。一个传感器节点的通信半径大约为 30 m, 通信范围在 5~50 m 变化。在该实验中, 节点的数量仍为固定的 50 个。如图 5 所示, 分析曲线和实验曲线一致。此外, 错误引发女巫攻击相关警报的概率极低, 低于 0.003 5, 这表明当通信半径改变时, 提出的检测方案的操作相对不变。

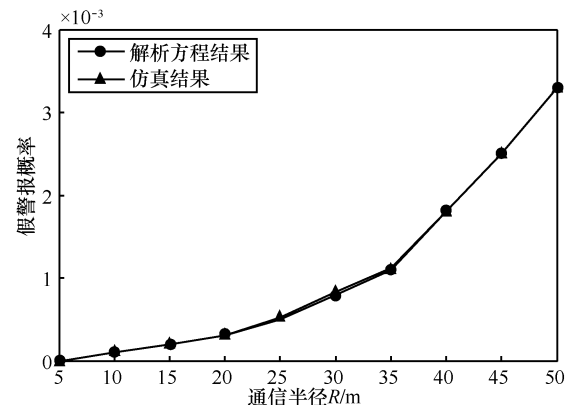


图 5 假警报概率与通信半径的关系

图 6 所示为提出算法受测距估算误差影响的程度, 测试到的最小测距估算误差为 30 cm, 并且该数值增加到 100 cm, 节点通信范围为 30 m, 节点的数量固定为 50 个。如图 6 所示, 测距估算误差影响了提出算法的检测准确度, 导致误报数量的线性增加。此外, 曲线显示了假警报概率没有超过 0.002 5, 属于安全范围。

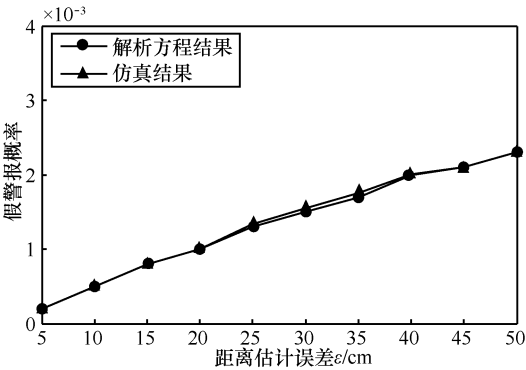


图 6 假警报概率与测距估计误差的关系

图 7 所示为节点密度对假警报概率的影响,节点密度表示部署区域的构成。实验中,进一步按比例缩小传感器区域来确定节点数量对算法功效的影响。每个节点的区域设置为 15 km^2 。例如,当节点数为 10 时,总传感器区域为 $10 \times 15 \times 10^3 = 1.5 \times 10^5$ 。其他所有参数为默认值 ($R=30\text{ m}$, $\varepsilon=30\text{ cm}$)。在这种场景下,假警报概率比之前实验中的要高。这种现象主要是因为潜在密集节点部署。当总面积为 1.65 km^2 的区域内有 110 个节点时,假警报概率几乎到达 0.046,很容易观察到节点数量增加的影响比扩展部署区域的影响更大。

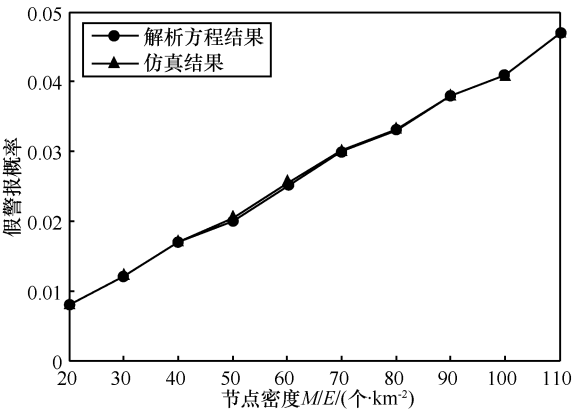


图 7 假警报概率与节点密度的关系

总之,基于 UWB 距离信息的女巫攻击检测算法即使在压制条件下仍能有效运行,在大多数情况下假警报概率保持在较低水平。另外,节点密度是影响错误发出女巫攻击相关警报的最关键因素。

4.3 仿真结果分析

在 WSN 中没有恶意活动的情况下,假警报概率反映出提出算法的性能。下面进行当合法和恶意节点共存于一个传感器区域内时的仿真测试。在所有研究场景中,由于女巫节点的位置也是一致选择的,所以恶意节点和合法节

点都不能知道彼此精确的位置。

由图 4~图 7 可知,FNR(false negative rate,假负率,也称为假警报概率)极低,大约为 0.01,产生了大约 100% 的检测准确度。该结果证明了提出的 PUWBD 在准确检测大规模 WSN 中女巫攻击方面的顽健性。

表 2 给出了当合法节点的数量 M 改变时,FPR(false positive rate,假阳性率)的结果。节点的数量在 10~110 个变化,女巫节点数量相当于总合法节点的 20%,在 2~22 变化,变化步长为 4,FPR 值仍旧很低,低于 0.006%。这说明提出的 PUWBD 没有受到 WSN 中合法节点和女巫节点数量的影响,同时也说明当节点数变大时,FPR 的值会增加。

表 2 改变节点数 M 时报告的假阳性率

节点数/个	FPR
10	0
30	0.001%
50	0.002%
70	0.003%
90	0.005%
110	0.006%

表 3 给出了通信半径变化时的 FPR。 R 在 5~55 m 变化,变化步长为 5 m,节点数量保持不变,为 50 个。总共考虑 10 个女巫节点,相当于总合法节点的 20%。节点通信范围的变化对 FPR 性能的影响很小。此外,FPR 随着通信半径的增加而增加。由于产生假警报的概率随着通信半径的增加而增加,所以上述推论在预料之中,即合法节点更有可能在相同共存区域内安排 2 个或多个合法邻居。即使 FPR 向上增加,但其最大值仍然很低(0.008%)。

表 3 改变通信半径 R 时报告的假阳性率

通信半径/m	FPR
5	0
15	0
25	0.001%
35	0.003%
45	0.005%
55	0.008%

表 4 给出了测距估算误差对 FPR 的影响。测距估算误差 ε 在 10~110 cm 之间变化,变化步长为 2。其他所有参数为默认值。合法节点数量为 50 个,所以女巫节点数为 10 个。获得的结果与之前的评论一致。记录的 FPR 值也很低,这表明女巫攻击均被发现。

表 4 改变测距估测误差 ε 时报告的假阳性率

测距误差/cm	FPR
10	0.001%
30	0.002%
50	0.002%
70	0.004%
90	0.004%
110	0.005%

表 5 给出了区域大小 E 变化所带来的影响。区域大小在 $1\sim 3\text{ km}^2$ 变化。当部署区域有限时,导致了较高的假警报概率,这是因为节点密度变得很高,并且容易使合法节点错误,引发假警报。然而,FPR 仍然很低,低于 0.025%。因此,即使在严格的网络区域部署中,提出的 PUWBD 仍然可以有效揭露活跃的女巫节点。

表 5 改变区域大小 E 时报告的假阳性率

区域/ km^2	FPR
1	0.025%
1.4	0.006%
1.8	0.002%
2.2	0.001%
2.6	0.001%
3	0

总之,结果证明提出的 PUWBD 可以容忍并发的女巫攻击数量的变化,可以成功处理同时发生、可延展的女巫攻击。虽然潜在女巫攻击检测算法会产生假警报,但是这些警报非常少,并且对整个网络性能及其一致性没有重要影响。

本文方法与引言中提到的几种方法的比较结果见表6,可以看出本文的 PUWBD 是完整 ADS、轻量级的,即计算代价低,能识别直接和伪造两种攻击类型。相比之下,本文

方法的综合性能最优。

5 结束语

处理女巫攻击是确保 WSN 安全的关键问题。本文针对 IEEE 802.15.4 对等传感器网络提出了一种基于 UWB 距离信息的异常检测系统。其核心思想是女巫攻击检测算法依赖于潜在 UWB PHY 的精密测距能力,从而准确及时地检测女巫攻击。且以分布式方法运行,如果确定了可疑节点的位置,那么每个传感器节点都能够引发警报。提出的方法可以检测女巫攻击而不引入集中处理或第 3 个可信网络实体,但通过孤立恶意节点和假的女巫节点提供防御威胁来源的机制。

由于传感器节点消耗的能量在网络生命周期中起到至关重要的作用,在 PUWBD 运行的情况下评估能量消耗也是未来一个重要的研究方向。另外,处理多个位置的多移动女巫攻击非常具有挑战性,这些都是未来的重点研究内容。

参考文献:

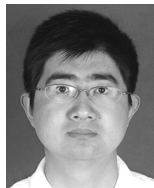
- [1] 余翔,刘磊,吴堃. 基于环形搜索的 WSN 簇间最优路由选择[J]. 电信科学, 2015, 31(2): 103-107.
XU X, LIU L, WU K. Optimal routing between clusters based on circular search method in WSN [J]. Telecommunications Science, 2015, 31(2): 103-107.
- [2] 李建中,高宏. 无线传感器网络的研究进展 [J]. 计算机研究与发展, 2008, 45(1): 1-15.
LI J Z, GAO H. Survey on sensor network research [J]. Journal of Computer Research and Development, 2008, 45(1): 1-15.
- [3] SANG S J, VALERO M, BOURGEOIS A, et al. Attacking and securing beacon-enabled 802.15.4 networks [J]. Wireless Networks, 2014, 21(1): 1-19.

表 6 不同女巫攻击检测系统的对比分析

类别	PUWBD 系统	参考文献[6]	参考文献[7]	参考文献[8]	参考文献[9]	参考文献[10]	参考文献[12]
完整 ADS	✓	×	×	✓	✓	×	×
轻量	✓	×	×	×	✓	✓	×
基于验证方法	×	✓	✓	×	×	×	✓
位置信息	✓	×	×	✓	✓	✓	×
支持移动	×	×	×	×	×	✓	×
转移	×	×	×	×	×	✓	×
分析验证	✓	×	×	×	×	×	×
通信方式	直接	直接	直接	直接	直接	直接	直接
识别类型	伪造与偷窃	伪造	偷窃	偷窃	伪造与偷窃	伪造	偷窃
操作	分布式	集中式	集中式	分布式	分布式	分布式	集中式

- [4] 胡蓉华, 董晓梅, 王大玲. 无线传感器网络节点复制攻击和女巫攻击防御机制研究[J]. 电子学报, 2015, 43(4): 743-752.
HU R H, DONG X M, WANG D L. Defense mechanism against node replication attacks and sybil attacks in wireless sensor networks[J]. Acta Electronica Sinica, 2015, 43(4): 743-752.
- [5] GUI J J, TAO Z, ZHANG Y S. Modeling and analyzing the sybil attack to ad hoc routing protocols [C]//2010 International Conference on Multimedia Technology (ICMT), Oct 29-31, 2010, Ningbo, China. New Jersey: IEEE Press, 2010: 1-5.
- [6] XING K, RIVERA M J, LI J, et al. Attacks and countermeasures in sensor networks: a survey [M]. Berlin: Springer, 2010: 251-272.
- [7] 张婷, 何泾沙. 基于抗局部攻击的无线传感器网络定位方法[J]. 北京交通大学学报, 2012, 36(3): 80-83.
ZHANG T, HE J S. An attack-resistant localization method in wireless sensor networks[J]. Journal of Beijing Jiaotong University, 2012, 36(3): 80-83.
- [8] 罗文俊, 高一峰. 基于位置的身份验证[J]. 吉林大学学报(工学版), 2012, 35(S1): 300-303.
LUO W J, GAO Y F. Location based authentication [J]. Journal of Jilin University(Engineering and Technology Edition), 2012, 35(S1): 300-303.
- [9] LI X L, WU M L. A shadowing-model-based scheme for sybil attack detection in wireless sensor networks [J]. Journal of Convergence Information Technology, 2013, 38(8): 609-616.
- [10] 张俊伟, 马卓, 马建峰, 等. 基于位置密钥交换的 UC 安全模型[J]. 计算机研究与发展, 2014, 51(2): 353-359.
ZHANG J W, MA Z, MA J F, et al. UC security model of position-based key exchange[J]. Journal of Computer Research and Development, 2014, 51(2): 353-359.
- [11] 章丽娟, 王清贤. 基于多视图的攻击分类体系 [J]. 计算机应用研究, 2010, 27(1): 255-258.
ZHANG L J, WANG Q X. Network attack classification architecture based on multi-view [J]. Application Research of Computer, 2010, 27(1): 255-258.
- [12] LU A, WANG W, DNYTE A, et al. Sybil attack detection through global topology pattern visualization [J]. Information Visualization, 2011, 10(1): 32-46.
- [13] 东尚清. 可调带宽低功耗超宽带 Gm-C 低通滤波器的研究与设计[D]. 上海: 复旦大学, 2013.
DONG S Q. Research and design for ultra wideband Gm-C low pass filter of tunable bandwidth low power consumption [D]. Shanghai: Fudan University, 2013.
- [14] NEWSOME J, SHI E, SONG D, et al. The sybil attack in sensor networks: analysis & defenses[C]//Third International Symposium on Information Processing in Sensor Networks, April 26-27, 2004, Berkeley, CA, USA. New Jersey: IEEE Press, 2004: 259-268.
- [15] SAHINOGLU Z, GEZICI S. Ranging in the IEEE 802.15.4a standard [C]//2006 IEEE Wireless and Microwave Technology Conference, Dec 4-5, 2006, Clearwater Beach, FL, USA. New Jersey: IEEE Press, 2006: 1-5.

[作者简介]



张衍志(1982-),男,四川工程职业技术学院讲师,主要研究方向为网络安全等。



叶小琴(1979-),女,四川工程职业技术学院讲师,主要研究方向为网络安全等。